SHIELD

03
AĞUSTOS
2018
FİYATI: 10 TL

Hızır Gibi Yetişen 10 Ünlü İnsan
O meşhur simaların bazıları kahraman! Hayat kurtaran 10 ünlünün hikayesi

GÜVENLİ YAŞAM REHBERİNİZ
SHIELD.COM.TR

Havuz Tehlikesi
Yüzme havuzları tehlike saçıyor! Riskler ve korunma yöntemleri

Katil Robotlar
Yeni yardımcılarımız bizi bir gün gerçekten öldürebilir mi?

DİJİTAL ÖLÜMSÜZLÜK

Sonsuz hayata ulaşmak için binbir yol deneyen insan, teknoloji sayesinde dijital ölümsüzlüğe belki de ilk defa bu kadar yakın!



SUÇ DOSYASI
Kâhin Teknoloji
Suçlar henüz meydana gelmeden önlenebilir mi?

DİJİTAL
Hack'lendim mi?
Cihazlarınızın hack'lendiğini anlamanın 8 yöntemi

GİZLİLİK
Şirketler Sizi İzliyor
Yaz tatilinde güvenliğiniz için bu tedbirleri elden bırakmayın



Exclusive

BİR İŞLETİM SİSTEMİNİN İÇİNDE YAŞAMAK



Ağustos sayımızda kapak konusu olarak çok eski bir hayali işledik: Ölümsüzlük! İnsan kadar eski bir fanteziden bahsediyoruz. Günümüzde ilk defa mantıklı bir açıklama ve bilimsel bazı yöntemler izlenerek insanlar ölümsüzlüğü mümkün kılmaya gayet ediyor. Üstelik bu çalışmalar milyonlarca liralık bütçelerle ve titizlikle sürdürülüyor. Bir hayalin peşinde koşanların neler yaptıklarını, geçmişten günümüze dijital ölümsüzlüğün hikayesini anlattık bu sayımızda.

Bilimkurgu edebiyatının ve sinemasının pek çok örneğinde, insanın dijital kopyasının oluşturulduğu işlendi. Bir defa yapabildikten sonra, teorik olarak sonsuz sayıda kopyanız üretilebilir. Fakat ne için?

Bedensiz yaşayabilir misiniz? Bedeniniz olmadan buna yaşamak denebilir mi? Bir rüyadaymışçasına, gerçek zamanda geçen birkaç saniyenin, sizin için birkaç bin yıl gibi geçtiğini hayal edin. Bir işletim sisteminin içinde, sonsuz zamanda, sizin gibi milyonlarca dijital kopya insanla, özel olarak yaratılmış dijital karakterlerle kurduğunuz iletişim ve paylaşımları düşünün. Şimdikine biraz benziyor değil mi?

Kim bilir, belki de diğer galaksilerde yaşamış ve bizden çok daha ileriye gidebilmiş canlılar vardı ve bedensiz olarak bir işletim sisteminin içinde yaşamayı seçerek fiziksel olarak yok olmayı tercih ettiler. Belki bir gün onlarla ancak bu koşullarda karşılaşabiliriz.

Ürkütücü bir senaryo gibi görünse de, gelecek nesiller için cazip bir teklif olabilir. Günümüzden sadece birkaç yüz yıl önce yaşayan insanların düşünme biçimlerini, hayat ve dünya hakkında sahip oldukları bilgiyi, yaşam tarzlarını bir aklınızdan geçirin. Ne kadar da büyük bir değişim!

Güvenli yaşam rehberiniz SHIELD, siz okuyucuları tarafından ilk iki sayısında büyük bir ilgiyle okundu. Bizi son derece memnun eden bu ilginin artarak sürmesi için elimizden geldiğince çalışıyoruz. Önümüzdeki aylarda çok daha fazlasını sunabilmek için bazı planlarımız var. İlginiz ve gönderdiğiniz e-postalar için teşekkürler.

Güvenle ve sağlıkla kalın...

Erdal Kaplanseren
Yayın Yönetmeni
erdal@layka.com.tr

Sahibi: Layka Medya Yayıncılık ve İletişim Danışmanlığı Dış Tic. Ltd Şti.
Yayın Yönetmeni: Erdal Kaplanseren **Görsel Yönetmen:** Hasan Kaya

Adres: Muradiye Mah. Kalıpçı Sok. No: 22/8 Beşiktaş/İstanbul **Tel:** 0212 972 9047 **Yazı İşleri:** bilgi@layka.com.tr
Reklam: reklam@layka.com.tr **Yayın Türü:** Yerel, süreli, aylık

İÇİNDEKİLER

Sayı 03 Ağustos 2018



Yetenekli yardımcılarımız olan robotlar birer katile dönüşebilir mi?



Kendilerini modern çağın Robin Hood'ları olarak tanıtan hacker'lar

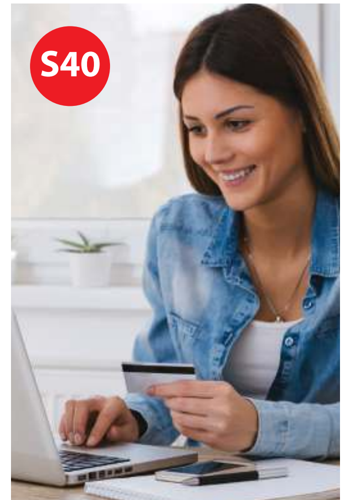


Yazı günlerinin keyfi olan yüzme havuzları pek çok hastalığa da ortam hazırlıyor. Havuzlardaki tehlikeleri ve korunma yollarını yazdık **S6**



Gelişmiş teknoloji sayesinde suçları ortaya çıkmadan engellemek mümkün olacak mı?







HAVUZLARDAN BULAŞABİLECEK Enfeksiyonlara Dikkat!

Sıcak yaz günlerinin vazgeçilmesi olan yüzme havuzları, **gerekli tedbirler alınmadığında** çok büyük bir tehdit

> Yaz aylarında kullanılan açık eğlence havuzların yanı sıra, spor amaçlı yüzme havuzları da sağlık konusunda onlarca farklı tehdidi içinde barındırıyor

Ortak kullanılan havuzlar sıklıkla ishal, mantar, idrar yolları, kulak ve göz enfeksiyonlarına sebep olabiliyor. Bu mikroplara karşı tedbirli olmak büyük önem taşıyor.

GÖZ ENFEKSİYONLARI

Yüzme havuzları, sıcak ve nemin etkisiyle bazı enfeksiyonların yayılımını kolaylaştırır. Havuz suyunun dezenfeksiyonunda yararlanılan klor bazlı maddelerin uygunsuz kullanımı tahrişlere, kornea yüzey bozukluklarına ve gözün bağışıklık sisteminin zayıflamasına neden olur. Belirtileri çapaklanma, kızarıklık, bulanık görme, kaşıntı, yanma ve batmasıdır. Gözlerinde enfeksiyon olan kişiler, diğer havuz kullananların sağlığını düşünerek bulguları düzelinceye kadar havuz kullanmamalıdır. Lens kullananların ise havuza lensleriyle girmemeleri uygun olur. Havuza lensleriyle giren kişilerde, şiddetli göz ağrılarının olması çeşitli enfeksiyonlardan dolayı olabilir. Bu nedenle havuza ya da denize girerken havuz gözlüğü kullanımı önemlidir.

SİNDİRİM SİSTEMİ ENFEKSİYONLARI

Havuzlardan bulaşan enfeksiyonların en başında, sindirim sistemi enfeksiyonları gelmekte ve bu durum





kendini bulantı ve/veya ishal ile kendini göstermektedir. Rotavirüs, Hepatit A, Salmonella, Shigella, E. Coli (Turist İshali) olmak üzere çok çeşitli virüs ve bakteriler su sirkülasyonu ve klorlamanın yetersiz olduğu havuzlarda uzun süre canlılığını koruyabildiği için bu mikropları içinde barındıran havuz suyunun yutulması ile ortaya çıkar.

GENİTAL BÖLGE VE İDRAR YOLU ENFEKSİYONLARI

Daha çok uygunsuz koşullara sahip havuzlardan kaynaklanan, idrar yolu enfeksiyonları ve kadınlarda görülen vajinit de sık rastlanan ve rahatsız edici enfeksiyonlar olarak karşımıza çıkar. Bu enfeksiyonlar idrar yaparken yanma, sık idrara çıkma, bel ve kasık ağrısı, genital bölgede ağrı, kaşıntı ve akıntı gibi belirtilerle kendini göstermektedir. Genital siğiller (HPV) de, havuzlardan bulaşabilmektedir.

DERİ ENFEKSİYONLARI VE MANTARLAR

Bazı deri enfeksiyonları ve mantarlar havuz yolu ile bulaşabiliyor. Bunların başında, genital siğiller ve 'molluskum kontagiozum' gelmektedir. Sıcak ile artan terlemenin, yaz aylarında mantar üremesini kolaylaştırdığı biliniyor. Aşırı miktarda klor kullanılan havuz suları, duyarlı bazı kişilerde ciltte tahrişe neden olabiliyor. Hijyenik olmayan ortamlardan ya da temiz olmayan havlulardan da uyuz, impetigo gibi deri hastalıkları bulaşabiliyor.



DIŞ KULAK YOLU ENFEKSİYONLARI VE SİNÜZİT

Dış kulak yolu enfeksiyonu, sulu ortamı seven bakteriler ve bazen de mantarların sebep olduğu bir durumdur. Şiddetli kulak ağrısı, kulakta akıntı ve işitme azlığı, kaşıntı ve ileri durumlarda kulakta şişme ve kızarıklığa neden olur. Uzun süre suda kalma ya da kulağa su kaçması sonucunda risk artar. Aynı zamanda suya dalma esnasında eğer varsa sudaki bakteriler burun yoluyla sinüslere kadar ulaşabilir ve sinüzite neden olabilir.

KORUNMAK YAPMANIZ GEREKENLER

- Klorlamanın ve su sirkülasyonunun yeterli olmadığını düşündüğünüz havuzlara girmeyin.
- Havuzda kesinlikle su yutmamaya özen gösterin. Özellikle sakız çiğnerken su yutulabileceği için, yüzerken sakız çiğnemeyin.
- Çocuk havuzu ve yetişkin havuzlarının ayrı olduğu tesisleri tercih edin.
- Islak mayo ile uzun süre oturmayın, mutlaka kurulanın.
- Havuzun bulunduğu kısma girmeden ayakların antiseptik solüsyonlar ile yıkandığı, havuza girmeden duş almanın ve bone kullanımının zorunlu olduğu tesisleri tercih edin.
- Havuzdan çıktıktan sonra hemen duş alarak üzerinizdeki olası mikrop ve fazla klordan temizlenin ve temiz çamaşırlar giyin.
- Havuzdan çıkar çıkmaz kurulanın. Çünkü bazı bakterilerin, uyuz ve mantar gibi enfeksiyonların gelişiminde nem, çok önem taşıyor.
- Havuza girerken mutlaka kulak tıkacı kullanın.
- Aktif bir kulak enfeksiyonunuz varsa ya da kulağınıza tüp takıldı ise havuza girmekten kaçının.
- Sinüzitten korunmak için havuza dalarken ya da suya atlarken burun tıkacı kullanın ya da burnunuzu elinizle kapatın.
- Göz enfeksiyonları açısından, havuz suyuyla teması en aza indirmek ve bu amaçla yüzücü gözlüğü kullanmak yararlı olur.



SORU-CEVAP

Telefonumu satarken güvenlik için neler yapmalıyım?

Elektronik cihazları yenisiyle değiştirme süresi her geçen gün biraz daha azalıyor. Eskiden çok uzun sürelerde değiştirdiğimiz hatta değiştirmek için bozulmasını beklediğimiz televizyon, bilgisayar ve diğer elektronik eşyaları daha bozulmadan kullanım ömrü dolmadan yenisiyle değiştirmeye başladık. Akıllı telefonlarda bu süre bir sene gibi çok kısa sürelere kadar düştü. Çoğu insan kullandığı telefonun yeni modeli çıktığı zaman eskisin satıp ya da bir yakınına verip hemen yenisini almaya çalışıyor. Bu da akıllı telefonlar açısından önemli bir gizlilik problemini de beraberinde getiriyor. Eski telefonunuzdaki hassas bilgileri yanlış ellere düşmemesi için tamamen silmeniz ve fabrika ayarlarına getirmeniz gerekiyor. Ancak unutmayın, ne kadar silseniz de fabrika ayarlarına getirseniz de eski telefonunuzdaki bilgiler bir şekilde ulaşılabilir olmaya devam edebilir. Örneğin silinen dosyaları kurtarmaya yarayan yazılımlarla geri alınabilir. Telefonunuzu satarken ya da bir başkasına verirken bunu asla unutmayın.

TELEFONUNUZU SİLMEDEN ÖNCE YAPMANIZ GEREKEN ÖNEMLİ ŞEYLER ŞUNLAR:

1. Telefonunuzdaki tüm verileri yedekleyin.
2. Telefonunuzda ekstra hafıza kartınız varsa çıkarmayı unutmayın
3. Google Authenticator gibi kimlik doğrulama uygulamaları kullanıyorsanız kullandığınız yerlerde devre dışı bırakıp yeni cihazdan etkinleştirmeyi unutmayın.



ANDROID

Cihazınız Android 5.0 ve sonrasını kullanıyorsa ve FRP (Factory Reset Protection – Fabrika Ayarlarına Sıfırlama Koruması) etkinse devre dışı bırakmayı unutmayın. Aksi takdirde telefonunuzu sattığınız ya da verdiğiniz kişi sizin Google hesabınız olmadan telefonu kullanamaz.

Android tabanlı cihazınızı fabrika ayarlarına döndürme adımları:

• Cihazınızın Ayarlar uygulamasını açın
• Sistem ardından Sıfırla (ya da Yedekle ve Sıfırla) seçeneğine dokunun. Gerekirse PIN kodunuzu, deseninizi veya şifrenizi girin. (bu ayarlar her telefonda aynı olmayabilir ancak benzer bir sürece sahiptir. Kesin adımlar için telefonunuzun kullanım kılavuzuna bakın)
• Fabrika verilerine sıfırla ardından Telefonu sıfırla seçeneğine dokunun. Gerekirse PIN kodunuzu, deseninizi veya şifrenizi girin.
• Cihazınızın dahili depolama alanındaki tüm verileri silmek için Her şeyi sil seçeneğine dokunun.
• Cihazınız silindiğinde, yeniden başlatma seçeneğini belirleyin.

Unutmayın, silinen verileri çeşitli dosya kurtarma uygulamalarıyla kurtarılabilir.

iPHONE

İphone'u fabrika ayarlarına döndürmeden önce bir başkasına satacaksanız veya verecekseniz Find My iPhone hizmetini devre dışı bırakmayı unutmayın. Bu işlemi Ayarlar > Adınız > iCloud > Find my iPhone kısmından yapabilirsiniz.

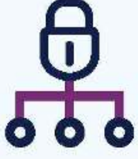
iPhone'nunuzu fabrika ayarlarına döndürme adımları

• iCloud'dan tamamen çıkış yapın. Bu işlemi Ayarlar > Adınız > Çıkış Yap kısmından yapabilirsiniz. Eğer iCloud'dan çıkış yapmadan telefonunuzu silerseniz, sildiğiniz veriler iCloud'dan da silinebilir. Buna çok dikkat edin.
• Tüm verileri silmek için Ayarlar > Genel > Sıfırla > Tüm İçerikleri ve Ayarları Sil kısmına gidin.
• Satacağınız veya vereceğiniz iPhone'un seri numarasını appleid.apple.com adresine giderek Apple hesabınızdan kaldırın.



10 Adımda Siber Güvenlik

Siber güvenlik konusunda şirketlerin ve bireylerin doğru adımları atması için ilk yapılması gereken, risklerin tanımlanması ve buna uygun siber güvenlik stratejisinin oluşturulması olmalı. Gözden geçirmeniz gereken siber güvenlik adımlarını listeledik.



Ağ Güvenliği
Ağlarınızı saldırılardan koruyun. Ağ çevresini savunun, yetkisiz erişimi ve kötü amaçlı içeriği filtreleyin. monitor ve güvenlik kontrollerini test edin.



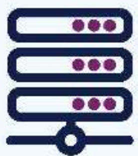
Kullanıcı eğitimi ve farkındalığı
Sistemlerinizin kabul edilebilir ve güvenli kullanımını kapsayan kullanıcı güvenlik politikaları üretin. Dahil etmek personel eğitiminde. Siber risklerle ilgili farkındalığı koruyun.



Kötü amaçlı yazılım önleme
İlgili politikaları üretin ve kuruluşunuz genelinde anti-malware savunmaları oluşturun.



Çıkarılabilir medya denetimleri
Çıkarılabilir medyaya tüm erişimi kontrol etmek için bir politika üretin. Medya türlerini sınırlayın ve kullanın. Kurumsal sisteme aktarmadan önce tüm ortamları zararlı yazılımlara karşı tarayın.



Güvenli yapılandırma
Güvenlik yamaları uygulayın ve tüm sistemlerin güvenli yapılandırmasını sağlayın. Bir sistem envanteri oluşturun ve tüm cihazlar için bir temel yapı tanımlayın.

Risk Yönetimi Sisteminizi Kurun
Yasal, düzenleyici, finansal ya da operasyonel riskler için, kuruluşunuzun bilgi ve sistemlerine ilişkin riskleri, aynı düzeyde olacak şekilde değerlendirin.

BANK

Kullanıcı ayrıcalıklarını yönetme
Etkin yönetim süreçleri oluşturmak ve ayrıcalıklı hesapların sayısını sınırlamak. Kullanıcı ayrıcalıklarını sınırlandırın ve kullanıcı etkinliğini izleyin. Aktivite ve denetim günlüklerine erişimi kontrol edin.



Olay yönetimi
Bir olay yanıtı ve felaket kurtarma yeteneği kurmak. Olay yönetim planlarınızı test edin. Uzman eğitimi sağlayın. Suç olaylarını kolluk kuvvetlerine rapor et.



Bunu başarmak için kuruluşunuz genelinde Yönetim Kurulu tarafından desteklenen bir Risk Yönetimi Rejimi yerleştirin ve üst düzey yöneticiler.

İzleme
Bir izleme stratejisi oluşturmak ve destekleyici politikalar üretmek. Tüm sistemleri ve ağları sürekli olarak izleyin. Saldırıya işaret edebilecek olağandışı etkinlik için günlükleri analiz edin.



Ev ve mobil çalışma
Bir mobil çalışma politikası geliştirin ve buna uymak için personeli eğitin. Güvenli temel çizgiyi uygulayın ve tüm cihazlara inşa edin. Verileri hem transit hem de dinlenme sırasında koruyun.



Hack'lendiğinizi Nasıl Anlarsınız?

Bilgisayarınızın garip davranışları size zararsız görünebilir ama aslında daha kötü ve sinsi bir durumun habercisi olabilirler. Güvenlik açıklarınızı nasıl teşhis edebileceğinizi ve bu durumları düzeltmek için neler yapabileceğinizi anlatıyoruz.

BELİRTİ 1:
SAHTE ANTİVİRÜS UYARISI

Nasıl anlaşılır? Ekranınızda beliren güvenlik mesajları yaptığınız işleri engeller ve bilgisayarınıza zararlı bir şeyler bulaşmış olduğu konusunda sizi uyarır. Bu mesajlardan bazıları aktivasyon kodu ister, bazıları da sisteminizde yüzlerce virüs bulduğunu iddia ederek onları temizlemeyi önerir. Bu uyarıların sahte olma ihtimali çok yüksektir, ama sahte bir antivirüs uyarısı görüyor olmanız da bilgisayarınıza gerçekten zararlı bir yazılım bulaştığının işaretidir.



Ne yapılmalı? Gördüğünüz uyarıda gerçek antivirüs programınızın adı yazıyor mu? Arayüz tasarımı gerçek antivirüs programınıza benziyor mu? İkisi de farklıysa veya sisteminize daha önce antivirüs yüklemediyseniz hiçbir şeye tıklamamaya özen gösterin. Bunun yerine inatla ekranınızda kalan pencereyi kapatmak için Ctrl+Shift+Esc tuşlarına birlikte basarak ulaşabileceğiniz Görev Yöneticisi'ni kullanın. Çalışan işlemler listesinde zararlı yazılımın adını bulun ve "Görevi sonlandır" diyerek kapatın. Ardından, eğer yapabiliyorsanız üzerinde çalıştığınız belgeleri kaydedin, sonra da bilgisayarınızı kaparatarak Güvenli Mod'da yeniden başlatın. (Güvenli Mod'a ulaşmak için bilgisayarınız açılırken F8 tuşuna art arda basın. Windows size Güvenli Mod'u önerecektir. Windows normal şekilde açılırsa tekrar deneyin.) Zararlı programı Denetim Masası'ndaki "Program kaldır" aracıyla kaldırmaya çalışın. Listeyi tarihe göre sıralamak, en son yüklediğiniz veya adı tanıdık gelmeyen programları kaldırmak faydalı olabilir. O da işe yaramazsa Malwarebytes Anti-Malware (**www.malwarebytes.org**) gibi zararlı yazılımları bulabilen bir programla tarama yapmayı deneyin. Daha sonra Başlat veya Başlangıç ekranına "rstrui" yazıp Enter'a basarak Sistem Geri Yükleme'yi çalıştırın bilgisayarınızı zararlı yazılımların bulaşmadığını düşündüğünüz bir tarihe döndürün. Ardından tüm sisteminizi gerçek bir antivirüs yazılımıyla tarayarak zararlı yazılımın bilgisayarınızda bıraktığı tüm izlerden kurtulun.

BELİRTİ 2
SOSYAL MEDYA VE E-POSTA SPAM'LERİ

Nasıl anlaşılır? Facebook sayfanızda birdenbire "Neler olduğuna inanmayacaksın!" diyen bir kadının fotoğrafları veya video görünümlü linkler görülmeye başladıysa, Twitter'da olağan tweet'lerinizin dışında reklam veya link içeren tweet'ler paylaşılıyorsa ve bunların hiçbirini siz paylaşmadıysanız bir sorun var demektir.

Web tabanlı e-posta hesabınız ele geçirildiyse arkadaşlarınız sizden gelen ve onlara şüpheli görünen ürün tavsiyeleri, İngilizce e-postalar veya dosya ekleri postalar alabilirler.

Ne yapılmalı? Maalesef bu tip hesap hırsızlıkları o kadar sık gerçekleşiyor ki ünlü web servisler hack'lenen hesaplar için uyulması gereken süreçler belirlediler. Bunları adım adım uygulayarak hesaplarınızı geri alabilirsiniz. Facebook için **www.facebook.com/hacked** adresli Hesabını Güvene Al sayfasına gidip adımları uygulayarak hesabınızdan gönderilen spam'leri durdurabilirsiniz. Twitter'ın önerilerini görmek içinse "Hesabım kontrolüm dışında hareket ediyor" sayfasına (**bit.ly/twitter204**) girin. Gmail hesabınıza erişemiyorsanız onun da kullanışlı bir "Güvenliği ihlal edilmiş Gmail hesabı" sayfası (**bit.ly/gmail204**) var. Benzer işlemler için Yahoo Mail'in (**bit.ly/yahoo204**) ve Outlook.com'un (**bit.ly/outlookcom204**) da ilgili sayfalarını kullanabilirsiniz.



BELİRTİ 3
HESABINIZIN PAROLASI DEĞİŞMİŞ

Nasıl anlaşılır? E-posta servisinize, çevrimiçi bir mağazaya veya en kötüsü banka hesabınıza girmeye çalışırken parolanızın yanlış olduğu veya parolanızın kullanıcı adınızla uyuşmadığı belirtiliyorsa bir şeyler ters gidiyor demektir.

Ne yapılmalı? Panik yapmadan ve kredi kartlarınızı kapattırmadan önce parolanızı doğru yazdığınızdan ve Caps Lock tuşunun



açık olmadığından emin olun. Çoğu servisin benzer şekilde çalışan bir "Parolamı unuttum" sayfası vardır. Bu sayfanın linki çoğunlukla kullanıcı adı ve parolanızı girdiğiniz kutuların yanında veya altında yer alır. Parolanızı hemen değiştirmek için bu bağlantıları kullanabilirsiniz. Eğer farklı hizmetlerdeki hesaplarınızda da aynı parolayı kullanıyorsanız onları da değiştirmeniz yararınıza olacaktır. Eğer bankanıza ulaşmakta zorluk çekiyorsanız en doğrusu telefonla müşteri hizmetlerine danışmak olacaktır. Bankalar sizin söylediğiniz kişi olup olmadığınızı doğrulamak için telefonda size çeşitli güvenlik soruları sorar. Bu soruları yanıtlayarak hesabınıza yeniden erişebilirsiniz.

BELİRTİ 4
TARAYICINIZDAKİ VEYA MASAÜSTÜNÜZDEKİ DEĞİŞİMLER

Nasıl anlaşılır? Web tarayıcınızı açtığınızda sizin ayarladığınızdan başka bir giriş sayfasıyla karşılaşıyorsanız, yeni bir araç çubuğu belirdiyse veya varsayılan arama motorunuz değiştiyse kuşkulanmaya başlayabilirsiniz. Masaüstünüzde veya bildirim alanında tanımadığınız bir simge

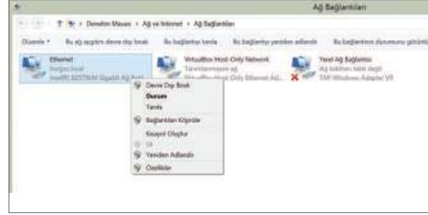
varsa, bilgisayar açılırken yeni bir program gizemli bir şekilde otomatik olarak çalışmaya başladıysa dikkatli olmanız gerekir. Bazen bu gibi şeyler kötü amaçlı yazılımlardan daha sinir bozucu olabilir, fakat aynı zamanda güvenliğinizin ihlal edildiği anlamına da gelebilir.
Ne yapılmalı? Çoğu web tarayıcısı istenmeyen eklentileri kaldırmanıza (en azından devre dışı bırakmanıza), giriş sayfanızı ve arama motorunuzu seçmenize izin verir. Ayrıca Windows Denetim Masası'ndaki "Program kaldır"ı kullanarak reklam amaçlı ürünlerden ve program deneme sürümlerinden kurtulabilirsiniz. Bilgisayarınızdan gitmemekte direnen şeyler için de bilgisayarınızı bir antivirüs taramasından geçirebilir, antivürüse ek olarak Malwarebytes Anti-Malware veya SUPERAntiSpyware programını (**www.superantispyware.com**) kullanabilirsiniz. Bazı programlar çok gizli şekilde çalışıp görünmez kalabilirler. Bilgisayarınızda bir şeylerin ters gittiğini ancak bilgisayarınız garip bir şekilde yavaşladığında anlarsınız. Microsoft'un ücretsiz Autoruns aracını (**bit.ly/autoruns204**) kullanarak hangi programların bilgisayar başlatılırken otomatik olarak açıldığını görebilir, onları devre dışı bırakabilir veya silebilirsiniz.



BELİRTİ 5
GARİP FARE DAVRANIŞLARI

Nasıl anlaşılır? Fare imleciniz kendi başına hareket ediyorsa, hatta sadece rastgele hareket etmek yerine belirgin bir şekilde bazı programları açıyor, web sayfalarına giriyor ve dosyalar içinde dolaşıyorsa bilgisayarınıza girilmiş demektir. Neyse ki bu şekilde gerçekleşen bilgisayar korsanlığı oldukça az.
Ne yapılmalı? Böyle bir durumla karşılaştığınızda karşınıza bir uzman olabilir. Bunu temizlemek için de bir uzmandan yardım almanız gerekebilir. Tabii hemen uygulamanız gereken birkaç basit ama önemli adım var. Öncelikle internet bağlantınızı kesin. Ağ kablonuzu çekebilir veya kablosuz ağdaysanız bildirim alanındaki ağ simgesine sağ tıklayın ve "Ağ ve Paylaşım Merkezi'ni Aç > Bağdaştırıcı ayarlarını değiştirin > Kablosuz Ağ Bağlantısı"na sağ tıklayıp "Devre Dışı Bırak" deyin. Kullandığınız tüm çevrimiçi servislerdeki parolalarınızı değiştirmeniz gerekecek çünkü hepsinin çalındığını varsayıyoruz. Parolaları değiştirmek için temiz olduğuna inandığınız başka bir bilgisayar kullanın. Son zamanlarda kredi kartınızla internetten alışveriş yaptıysanız onu da iptal emeniz gerekebilir.

Sorunlu bilgisayarınızı Güvenli Mod'da tekrar başlatın, bir antivirüs programı çalıştırın ve Sistem Geri Yükleme'yi kullanarak bilgisayarınızı geri alın. İnternet bağlantınızı tekrar kurarak aynı şeylerin olup olmayacağına bakın. Eğer aynı şeyler devam ederse bir uzmandan teknik destek almanızı öneririz. Ekranınızda gelişen olayları telefonunuzla videoya geçmek, sorunu anlatmak açısından iyi bir yöntem olacaktır.



BELİRTİ 6
DEVRE DIŞI BIRAKILMIŞ GÜVENLİK VE SİSTEM ARAÇLARI

Nasıl anlaşılır? Antivirüs programınızı veya Görev Yöneticisi ve Kayıt Defteri Düzenleyicisi gibi Windows araçlarını açamıyorsanız, bu programlar hata



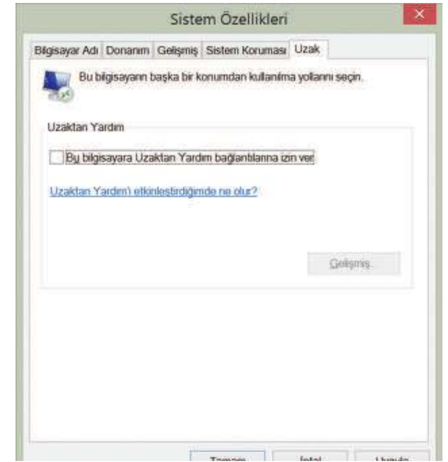
veriyorsa dikkatli olmalısınız.
Ne yapılmalı? Sistem Geri Yükleme aracı çalışıyorsa ilk yapmanız gereken sistemi geri almayı denemek olmalı. Ayrıca Güvenli Mod'da bilgisayarı açıp antivirüs taramasını oradan yapıp yapamadığınıza da bakabilirsiniz. Ücretsiz Norton Power Eraser (**www.norton.com/npe**) gibi bu konuda uzmanlaşmış bir aracı kullanarak da bilgisayarınızda sorun yaratan gizli tehditleri ortaya çıkarabilirsiniz.

BELİRTİ 7
BİRİ SİZİ İZLİYOR

Nasıl anlaşılır? Web kameranızı çalıştıracak bir şey yapmamanıza rağmen kameranın çalıştığını gösteren ışık yanıyorsa ortada bir sorun vardır. Bu şekilde gerçekleşen uzaktan erişim korsanlıkları maalesef yaygın ve haberlere de konu oluyorlar.



Mahrem görüntüleriniz sizden habersiz kaydedilerek şantaj malzemesi bile yapılabilir.
Ne yapılmalı? Öncelikle kameranızın üzerini kapatın. Bilgisayarınız yeniden başlatın ve Windows Gezgini'ni açıp Bilgisayar'a (Windows 8.1'de "Bu bilgisayar") sağ tıklayın, Özellikler > Gelişmiş sistem ayarları > Uzak sekmesindeki "Bu bilgisayara Uzaktan Yardım bağlantılarına izin ver" işaretini kaldırın ve Tamam'a tıklayın. Ardından antivirüs ve antispyware programlarıyla tarama yaparak suçluyu bulup temizlemeye çalışın.



BELİRTİ 8
MİCROSOFT'TAN(!) GELEN TELEFON

Nasıl anlaşılır? Sizi Microsoft'tan aradığını iddia eden ve bilgisayarınızda birtakım sorunlar olduğunu söyleyen kişilerden şüphelenmenizde fayda var. Arayanlar probleminizi ortadan kaldırmak için size yardım etmek istediklerini söyler ve genellikle sorunu tanımlamaya yarayan bir yazılımı yüklemeniz için size verecekleri bir adrese girmenizi isterler.
Ne yapılmalı? Bu durum bilgisayarınızın gerçekten tehlike altında olduğunu söylemekten daha çok, bir dolandırıcılık ve bilgisayarınıza ulaşılmaya çalışıldığını haber veren bir işarettir. Telefonu kapatın ve sizden yapmanızı istedikleri hiçbir şeyi de yapmayın. Microsoft asla siz talep etmedikçe bilgisayarınızı onarmanıza yardım etmek adına sizi telefonla aramaz (**bit.ly/telefon204**). Unutmayın ki dolandırıcılar siz onlara giriş izni vermeden bilgisayarınıza uzaktan erişemezler. Telefonda sizden parola, kredi kartı vb. isteyen veya bir adrese girmenizi söyleyen hiç kimseye inanmayın. ■





DİJİTAL ÖLÜMSÜZLÜK MÜMKÜN MÜ?

Ölümlü olduğunu anladığından beri insanoğlunun keşfetmek için binbir yol denediği ölümsüzlüğe, teknoloji sayesinde belki çok yakınız. Dijital ölümsüzlük mümkün mü? Belki bu yazı, bu konuda fikrinizi değiştirecek.

Yazar: Erdal Kaplanseren



Yaklaşık 15 yıl önce, Milliyet'te teknoloji üzerine yazdığım yazılarımdan birinde bu konuya değinmiş ve dijital ölümsüzlüğün mümkün olabileceğini, bilim insanlarının henüz özellikle bu konuda çalışmasa dahi, diğer alanlardaki gelişmelerin bunu doğuracağını söylemiştim.

Peki ne zaman? Kahve falı bakar gibi 3 ay mı desem, 3 yıl mı desem diye yuvarlak tahminlerde bulunmayacağım elbette. Günümüzde kullandığımız ve yakın zamanda daha etkin biçimde yaşamımızı etkileyecek bazı teknolojiler, dijital ölümsüzlüğün kapılarını aralayacak. Benim kişisel tahminim, 2050 yılına kadar dişini sıkıp ölmemeyi başaranlar için iyi haberlerimiz olabilir.

HAYAL EDİN, GERÇEK OLSUN

Beyninizin dijital bir sürümünün "bulut"ta (güvenli ve internette her an bağlı bir sunucuda) bulunduğunu ve anlık olarak yaşadıklarınızla senkronize edildiğini düşünün. Elektrik sinyalleri sayesinde materyalize ettirdiğiniz bilinciniz, sentetik bir beyinde ve yapay bir bedende depolanabilecek. Teorik olarak bu şekilde sonsuza kadar yaşayabilirsiniz. Çünkü benliğinizi taşıyan bir bedeniniz olmayacak. Daha doğrusu istediğiniz herhangi bir yapay beden size ait olabilecek. Ve dünyanın neresinde isterseniz! Hatta uzayda bile! Tek yapmanız gereken, olmak istediğiniz yapay benden içine "siz"i yüklemek olacak.

Biraz daha ileriye giderek, uzak gelecekte, "beden"in günümüzdeki anlamını tamamen yitireceğini, kullanacağımız bir eşyaya dönüşeceğini iddia edebilirim.

GENÇLİK İKSİRİNDEN DİJİTAL ÖLÜMSÜZLÜĞE

Ölümsüzlük arzusu çok eskilere dayanıyor. Milattan Önce 3. yüzyıldaki antik Çin, cıvanın ölümsüzlüğün

Ölümsüzlük veya gelecekte tekrar diriltilme konusunda çalışmaların geçmişi onlarca yıl öncesine dayanıyor

anahtarı olduğuna inanıyordu. Rivayete göre Çin'in ilk imparatoru Kin Şi Huang, sonsuz yaşam için bu uğurda yüksek miktarda cıva tüketti ve 39 yaşında cıva zehirlenmesinden öldü.

Günümüze geri geldiğimizde ise karşımıza Martine Rothblatt çıkıyor. Telekomünikasyon avukatı, yönetici ve hem Sirius XM uydu radyosu hem de United Therapeutics biyoteknoloji firmasının kurucusu olan Rothblatt'a göre ölüm bir son değil; bir seçenek. Bir "transhumanist" olan bu iş kadını, ayrıca Terasem Hareketi'nin de kurucusu. Henüz yaratılmamış, bildiğiniz her şeyi bilen ölümsüz avatarınızın, kısaca siber benliğinizin hakları konusunda şimdiden endişeleri bulunuyor. Bunu, yani siber benliğinizi, kişiliğinizin bir simülasyonundan ziyade bir emülasyonu olarak düşünün.

2045 İNİSİYATİFİ VE AVATAR PROJESİ

Kişisel, ucuz ve gerçekçi avatarların geliştirilebilmesinden önce, insan beyninin yapısal haritasının çıkarılması gerekiyor. Sinirsel bağlantılar, sinirsel yapılar ve her birinin fonksiyonlarının deşifre edilmesi bir ön koşul. Ayrıca elektrik sinyallerinin koda dönüştürülmesi ve sonsuz benliğinizi çalıştırabilecek donanımın da geliştirilmesine ihtiyaç var.

Rus girişimci ve dolar milyoneri Dimitri İskov'un "2045 İnisiyatifi" adını verdiği bir projenin şemsiyesi altında yürütülen "Avatar Projesi" de bir başka güncel çalışma olarak öne çıkıyor. Şu ana kadar milyonlarca dolar harcanan proje dört safhadan oluşuyor. Sürecin birinci safhasını oluşturan Avatar A'da, insan beyni tarafından yönetilebilen bir robot geliştirilecek. Avatar B, insan beynini sentetik bir bedene nakletmeyi içeriyor. Avatar C'de, biyolojik beynin içeriği sentetik yedeğine yüklenecek. Avatar Projesi'nin son ayağı olan Avatar D'yi ise emülasyon aşaması oluşturuyor: Biyolojik bedeni ve beyni, insan bilincinizin dijital sürümüne ev sahipliği yapacak bir hologram ya da bir diğer avatar ile değiştirmek.

KARBON KOPYA PROJESİ

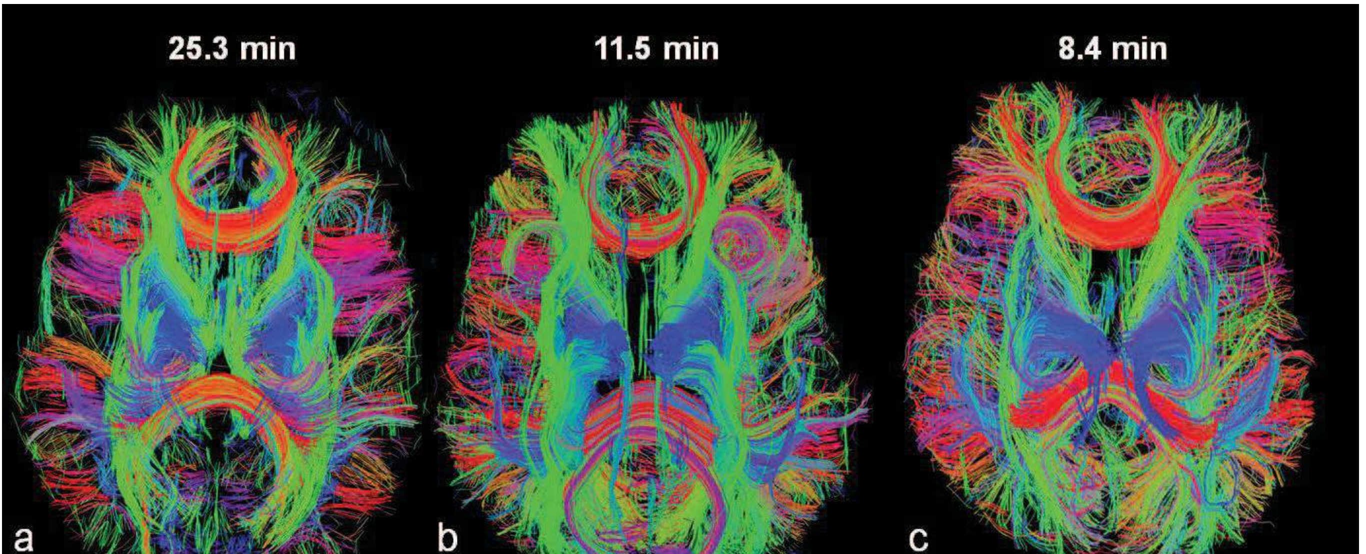
Sinirbilimci Randal Koene tarafından 2012'de kurulan Carboncopies.org da günümüzün önemli projelerinden bir başkası ve Dimitri İskov, 2045 İnisiyatifi için bu projeyi destekliyor. Ticari amaç gütmeyen bu organizasyonun kökleri 2007'ye kadar uzanıyor. Koene'nin liderlik yaptığı transhümanizm savunucuları, dijital ölümsüzlüğü aktif bir şekilde desteklemeye çoktan başladılar. Eksiksiz beyin emülasyonu fikrinin temelini bizzat bu idealistler attı. Grup ayrıca insan beyninin taklit edilebilmesinden önce çözülmesi gereken önemli adımların taslağını da çıkardı. Bunun içinde, insan beyni yapısını haritalamak, sinir bağlantılarını ve işlevlerini çözmekle beraber, bir bilgisayar yongasının silikonundaki ölümsüz kişiliğinize ev sahipliği yapacak yazılım ve donanımın geliştirilmesi de bulunuyor.

Elbette Google da bu konuda boş durmuyor. Arama motoru olarak hayatımıza giren ve şu aralar sürücüsüz otomobil ve robotlarla kafayı bozmuş olan Google, 2012'de Google Brain projesini başlatmıştı. Domestik bir araştırma projesi olan Google Brain, daha çok makine öğrenimi üzerinde yoğunlaşıyor. Ne de olsa makinelerin, gerçek anlamda bir insan gibi olması için çok şey öğrenmeleri gerekiyor.

İNSAN CONNECTOME PROJESİ

Bilim insanları, farklı dallarda yürüttükleri araştırmalarda her geçen gün yeni bir keşifte bulunuyor. İnsan Genom Projesi, insanın tüm genlerini tanımlamak ve DNA'sını sıralamak için başlatıldı ve oldukça önemli sonuçlar verdi. İnsan Microbiome Projesi ise insan bağırsağında yuvalanan tüm mikropları tanımlamak ve sıralamak için başlatılmıştı. Diğer benzer bir bilimsel araştırma projesi ise insanlığımızı birebir temsil eden başka bir şeyi

Dünyanın farklı ülkelerinde birbirinden bağımsız ama iletişim halinde süren pek çok dijital ölümsüzlük projesi var



Human Connectome Project, dijital ölümsüzlük için bir ön koşul olan, insan beyninin çözümlenmesi adına önemli bir çalışma.



tanımlıyor, haritalıyor ve çözümlüyor. İnsan beyninin sinir hatlarını çıkaran bu projenin adı "İnsan Connectome Projesi".

Connectome'un, sizi kendiniz yapan şeylerden sorumlu olduğuna inanılıyor. İnsan beyni yaklaşık 100 milyar sinir barındırıyor. Bunların her biri, 10 bin civarında başka sinire mesaj gönderiyor. Sinyalleşmeyle beyin, bilgiyi şifreliyor, işliyor ve çağrıştırma oluşturuyor. Aynı zamanda muhtemelen insan olmanın özünü; kişisel anılarınız, yetenekleriniz ve sizi siz yapan tüm acayip özellikleri içeriyor. Bunların hepsi size ait connectome içinde yer alıyor.

İnsan bilinci kavramı genellikle bir arabanın anahtarlarıyla örneklendirilir. Arabanız harika bir makinedir ama ateşleme anahtarı olamadan kıvılcım oluşmaz ve çalışmaz. Bilinç, hem kendimizi hem de çevremizdeki dünyayı nasıl bildiğimiz, nasıl yaşadığımızdır ve beynimizin sinir ağında gerçekleşen bilgi alışverişinden oluşur.

İnsan bilincinin nasıl oluştuğuna dair birkaç teori rağbet görüyor. Örneğin, bütünleşik bilgi teorisinin savunucuları, sinir ağındaki bütünleşik bilginin miktarını "fi" isimli bir nicelik ile hesaplıyor. Ağ içinde ne kadar çok bağlantı varsa, o kadar çok bilgi paylaşımı yapılıyor. Bir başka teori ise insan bilincinin bir bilgisayar hafızası gibi çalıştığını öne sürüyor. Bütünsel çalışma alanı teorisi, bilinci, beynin bilgiyi toplama ve tüm sinir ağı boyunca dağıtma işlevinin bilincin ta kendisi olabileceğini iddia ediyor.

SOLUCAN ROBOTLAR İPUCU OLABİLİR Mİ?

Eksiksiz beyin emülasyonu araştırması alanındaki bilimciler, yuvarlak solucanların (Caenorhabditis elegans) 302 sinir ve 7 bin sinir bağlantısıyla beraber tüm sinir ağlarını başarılı bir şekilde haritaladılar. Sonraki aşamayı solucan beynindeki sinir ağı ve bağlantıları temel alan model üzerinden kod yazmak ve kodu bu örnekte olduğu gibi bir robota aktarmak oluşturuyor. Donanım olarak burnunun ucunda sonar sensor bulunduran robot solucan, biyolojik solucanın sinir hatlarını taklit eden motor sinirler barındırıyor.

Aynı işlem teorik olarak insan beyni için de uygulanabilir. Ama çok daha büyük ölçekte… İnsan beyninde yaklaşık 100 milyar sinir ve bu sinirler arasında da 100 trilyon bağlantı bulunur. Yoğun, şehir sokaklarını andıran insan beyni şebekesini haritalayıp sinir ağının kurallarını çözerek pek tabi nörolojik, nörodavranışsal ve nöropsikiyatrik hastalıkların kökleri hakkında tahmin edemeyeceğimiz ölçüde bilgiye ulaşabiliriz. İlaveten, beynin sinir bağlantılarıyla

ilgili bozuklukları önleme ve tedavi etme çalışmalarına paha biçilemez değerde bir ışık tutabilir. Ayrıca nasıl düşündüğümüz ve sonuç çıkardığımız, kendimizi nasıl algıladığımız hakkında derin bir anlayış kazanabilir ve aklımızı nasıl taklit edebileceğimizin yollarını bulabiliriz.

YAPAY ORGANLAR BEYNE TANIMLANABİLİYOR

Bilinç yükleme ya da kimyasal-bağımsız zihinlerin gerçekleşebilmesi için aklınızdaki her şeyin yeni bir sentetik beyne aktarılması gerekiyor. Bu dijital kopyanız, sadece hafızanızı değil, beraberinde sizi siz yapan kişiliğinizi ve bilincinizi de kapsıyor. C. Elegans araştırması henüz başlangıç aşamasında. Ama bilimciler yakın bir zaman için solucanın sentetik bir sürümünü geliştirmeyi planlıyor.

Öte yandan da DARPA'nın (Defansif İleri Araştırma Projeleri Ajansı) kendi Avatar Projesi bulunuyor. Pentagon'un bu projesi dahilinde uzaktan yönetim araştırmaları yapılıyor. Kısaca bu projenin amacını, gerçek askerlerin uzaktan yönetebildiği vekil askerler geliştirmek olarak tanımlayabiliriz.

Yine DARPA tarafından finanse edilen bir başka araştırmada, beyin implantları sayesinde uzuvlarını kaybetmiş kişiler, zihinlerini kullanarak protezlerini hareket ettirmeyi başardılar. İzlanda'da yürütülen benzer bir projede de amputeler, beyinlerine yerleştirilen 5 milimetre uzunluğunda ve 3 milimetre genişliğindeki sensörler sayesinde protez ayaklarını hareket ettirebildiler. Bu algılayıcılar, bacağın kalan kısmındaki kasları uyararak ve kontrol ederek çalışıyor.

Gelecekte, bedensiz biçimde, bir işletim sistemi içinde yaşama fikri kulağınıza nasıl geliyor?

SİZ DİJİTAL OLMAYI TERCİH EDER MİSİNİZ?

Dijital ölümsüzlüğe inanmayanların çoğu, fikrin prensiplerini her açıdan eleştiriyor. Şüphesiz dijital ölümsüzlük, doğrudan ciddi ahlaki ve etik sorunlar doğuracaktır. Belki de en önemlisi, toplumsal hayatta ciddi mahremiyet problemleri çıkarabilir. Örneğin, anıların hakları var mıdır? Peki anılar mahkemede delil olarak gösterilebilir mi? Bir başka problem de beyin nakli üzerinde kara bir bulut gibi geziniyor. Bazı bilimciler, başarılı bir insan beyni nakli için beyinle beraber omuriliğin de taşınması gerekebileceği yönünde uyarıyor ki bu durum işleri daha da karmaşık hale getiriyor.

Ölümsüzlük fikrine karşı çıkanların bir başka iddiası ise yapay beynin bir bilinci, gerçekten doğru biçimde temsil edip edemeyeceği yönünde. Bu konuda belki en dikkat çekici açıklamayı Seattle'daki Allen Sinirbilim Enstitüsü'nün baş bilimcisi Christof Koch söyledi: "Hava durumu bilgisayarda taklit edilebilir ama asla ıslaklık olmaz." Koch gibi düşünenler, insan beyninin bir bilgisayar çipi içinde taklit edilemeyeceğini, çünkü biyolojik beynin aksine, bir emülasyonda tahmin edilemez davranışlar ve doğrusal olmayan etkileşimler gibi karakteristik insan özelliklerinin bulunamayacağını ifade ediyorlar.

Peki, diyelim ki ömrünüz vefa etti ve dijital ölümsüzlüğün mümkün hale geldiği bir döneme ulaştınız. Bunu satın alır mısınız? Tüm benliğinizi, anılarınızı, hislerinizi oluşturan o dev kütüphanenizin bir bilgisayarın diskinde durması sizi nasıl hissettiriyor? Belki bunları düşünmek için erken fakat kabul etmeliyiz ki dijital ölümsüzlük, üzerine konuşulabilecek kadar da yakın.



Online Güvenlik İçin 35 İpucu

İnternet, tıpkı elektrik ve su gibi hayatımızın her alanda en önemli parçalarından biri haline geldi. Online dünyada her şeyin kontrolünüz altında ve güvende olması için mutlaka bilmeniz gereken güvenlik ipucu ve sırlarını paylaşıyoruz.

İnternete girdiğinizde herkesin peşinizde olduğu hissine kapılabilirsiniz: Verilerinizi satarak para kazanmayı uman sanal suçlular, ticari girişimlerinizi rehin alan sanal eylemciler ve e-postalarınızı kurcalayan devlet kurumları... Kötü adamlar giderek daha becerikli hale geliyorlar, ama kendini geliştiren sadece onlar değil. Hacker'lara karşı yöntemler geliştiren araştırmacılar ve güvenlik firmaları, tehditler karşısında daha akıllı çözümler getiriyorlar. Bu arada kullanıcılar da artık daha bilinçli hareket ediyor. Saldırılar daha incelikli hale gelip sıklaştıkça pratik savunma teknikleri öğrenme ihtiyacı da kendini daha çok hissettiriyor.

Mükemmel koruma diye bir şey yoktur ama tehditlerin sayısını azaltmak için de karmaşık ve pahalı yöntemler gerekmiyor. Süreçlere, sistemlere ve kişilere uygulanacak basit güvenlik önlemleri alarak saldırıların pek çoğunu engellemek mümkün. Diğer bazı saldırılar ise biraz daha uğraşmayı gerektiriyor. Artık güvenlik konusunu ciddiye almamız, savunma ufkumuzu genişletmemiz gerekiyor. Bu hızlandırılmış güvenlik eğitimi sayesinde sosyal ağlardan mobil cihazlara ve buluta kadar her alanda saldırganlardan uzak durmayı başaracaksınız.

TEMEL BİLGİLER: BİLİŞİMİN OLMAZSA OLMAZLARI

Mutlaka bilmeniz gereken güvenlik ipucu ve sırları paylaşıyoruz.

En temel önlemleri almazsak hiçbir yere varamayız. Aşağıdaki 12 maddenin hepsini uygulamıyorsanız önce bunları halledin ki diğer maddelerin anlamı olsun.

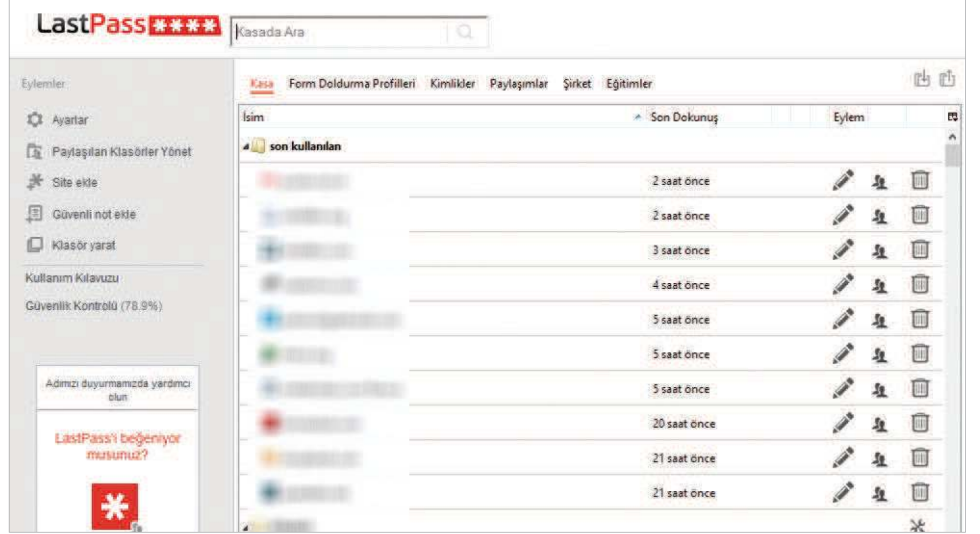
1 Verilerinizi düzenli olarak yedekleyin ve güvenli bir şekilde saklayın.

2 İşletim sisteminiz ve yazılımlarınız için yayımlanan güncellemeleri asla ihmal etmeyin.

3 Masaüstü işletim sisteminizin güvenlik duvarını kullanın. Orada olmasının bir nedeni var!

4 Zayıf parolalar kullanmamaya çalışın ve asla ama asla aynı parolayı birden fazla sitede kullanmayın. Parola yönetim yazılımlarından (örn. LastPass) faydalanın.

5 Mümkünse iki faktörlü kimlik denetimi (2FA) kullanın. Böylece, örneğin parolanızı yazdıktan sonra telefonunuzda oluşan kodu da girmeniz gerekir. Çoğu popüler servis bu özelliği sunar.



6 Veri aktarımı yaparken (e-posta da dahil) güvenli web bağlantıları kullanın. Adres çubuğunda asma kilit simgesinin göründüğünden emin olun.

7 Gizliliğinizi korumak ve güvenlik açıklarını engellemek için cihazlarınızı elden çıkarırken verileri sildiğinizden emin olun.

8 Antivirüs/antimalware koruması yükleyin ve onu sürekli olarak güncelleyin.

9 Güvenlik tehditlerinden ve yeni gelişmelerden haberdar olun. Ne de olsa bilgi güçtür!

10 Yönetici hesaplarında "admin" dışında bir kullanıcı adı kullanın. Varsayılan hesap olarak bu ayrıcalıklı hesapları kullanmayın.

11 Oturum açtığınız cihazları sahipsiz bırakmayın.

12 Windows'ta Otomatik Çalıştır/Otomatik Yürüt özelliğini kapatın.

GÜVENLİ SOSYAL AĞ

Firmalar tarafından pazarlama ve destek amacıyla da kullanılan sosyal ağlar artık sadece sosyal değiller. Giderek daha fazla sayıda insan herkesle her yerden bağlantıya geçmek fırsatını kullanıp en gizli bilgilerini paylaşıyor. Elbette bu arada risk de artıyor.

13 Varsayılan ayarları kullanmayın

Sanal suçluların en hoşuna giden şey, işlerini yaparken mümkün olduğu kadar az direnişle karşılaşmaktır. Sosyal ağlarda en az direniş gösterenlerse varsayılan güvenlik ve gizlilik ayarlarını kullananlardır. Ayarları kötü adamlara değil, size hizmet edecek şekilde değiştirin. Paylaşımlarınızı ve kişisel ayrıntılarınızı kimlerin görebildiğini hesaba katın. Hassas bilgileri herkese açık bir şekilde paylaşmak yerine oluşturacağınız paylaşım gruplarını kullanın. Çalıştığınız yeri ve işinize dair her şeyi profilinize yazarak kimlik avcılarının, özellikle de hedefli ve uzun süreli saldırılar gerçekleştirenlerin işini kolaylaştırmayın.



Bu "sosyal mühendisler", Facebook ve LinkedIn üzerinden firma araştırmaları yürüterek kapalı kapıları zorlayabiliyorlar. Sosyal ağlarda gezinirken arkanızda bıraktığınız ayak izleri, şirket ağlarına sızmak için izlenecek bir yol sunabilir. Kötü adamların işini kolaylaştırmayın.

14 Dostlarınızı tanıyın

Aslında söylemeye bile gerek yok: Yabancılarla konuşmayın, arkadaşlarınızı tanıyor olsalar bile! Listenizdeki kişiler güvenliği sizin kadar ciddiye almıyor ve her arkadaşlık isteğini kabul ediyor olabilir. Burada önemli olan sürekli dikkatli olmak. Bu nedenle arkadaşlık isteklerini özenle inceleyin.

15 Eski paylaşımlarınızı gözden geçirin

Eğer çok uzun süredir bir sosyal ağ hesabına sahipseniz, üç altın kuralı uygulayın: Gözden geçir, temizle, sağlama al. Büyük ihtimalle eskiden güvenliği şimdiki kadar ciddiye almıyordunuz. Paylaşımlarınızı gözden geçirin ve güvenli görünmeyen her şeyi silin.

Zaman Tünelindeki Eski Gönderilerin Hedef Kitlesini Sınırla

Bu aracı kullanırsan, zaman tünelinde arkadaşlarının arkadaşları ile veya herkese açık paylaştığın içeriklerin gizlilik ayarı Arkadaşlar'a değişecektir. Hatırlatma: Etiketlenen kişiler ile bu kişilerin arkadaşları bu gönderileri görebilecektir.

Ayrıca gönderilerinin her birinin kendi hedef kitlesini belirleyebilirsin. Tek yapman gereken, değiştirmek istediğin gönderiye gidip farklı bir hedef kitle seçmektir.

Eski gönderileri nasıl değiştirebileceğini öğren

Eski Gönderileri Sınırla

AĞDA GÜVENLİK

Pek çok sanal suçlunun peşinde olduğu şey size ait verilerdir. Bunlara giden yol olan ağınız da öncelikli hedeftir. Ayrıca saldırganlar bir DDoS saldırısıyla ağınızı işlemez hale getirebilir, ardından da saldırıya son vermek için fidye talep edebilirler.

16 Açık portları sınırlandırın

Kullanılmadığı halde açık olan portları (bağlantı noktalarını) tespit edip kapatın. Belirli hizmetlere ayrılan bağlantı noktalarını kapatmak akıllıca bir fikir. Öte yandan kullanılmayan portlar, saldırganların kolayca istismar edebilecekleri bir varsayılan yapılandırmaya dayanır. İsterseniz kafa karışıklığı yaratıp güvenliği artırmak ve otomatik sıfır gün saldırılarının çoğundan korunmak için bazı hizmetleri varsayılanlar dışındaki portlara yükleyebilirsiniz.

17 Veri akışınızı haritalayın

Çok da pahalı olmayan (hatta bazı durumlarda ücretsiz olan) ağ trafik akışı analizleri kullanarak ağınızda yolculuk eden verilerin haritasını çıkartın. Hangi verinin ne zaman nereye gittiğini bilirseniz, beklenmedik bir noktadan ağa giriş yapan birkaç gigabayt veri gibi sıra dışı etkinlikleri tespit edebilirsiniz.



Kullanılmayan portları kapatan bir güvenlik duvarı kullanın.

18 DDoS saldırılarından korunun

Trafik akış analizi, DDoS saldırılarından korunmanıza yardımcı olabilir. Sıra dışı bir trafik tespit edildiği anda gerekli filtre (atanmış bir cihaz veya web uygulaması güvenlik duvarı) harekete geçerek hareketliliği engelleyebilir. Bu tüm DDoS saldırılarında işe yaramayacaktır. Bu nedenle bulut tabanlı bir DDoS savunma sistemi alabilir veya servis sağlayıcınıza danışabilirsiniz. Bu hizmetler ne yazık ki ücretsiz değiller ama daha düşük altyapı harcamaları ve destek yatırımları gerektirmeleri nedeniyle, sıfırdan yerinde bir DDoS savunması kurmaktan daha ucuza mal olacaklardır.



Daha sağlam güvenlik için modeminizin yazılımını yükleyin.

19 Arabiriminizi kilitleyin

Ağa bağlı yazıcıların ve fotokopi makinelerinin web tabanlı yönetim arabirimleri olabilir. Bunların herkese açık olmadığından emin olun. Bu cihazlar, özellikle de küçük işletmelerde genellikle gözden kaçarlar. Örneğin web sunucunuz, soran herkese kimliğini bildiriyor mu?

Varsayılan ayarları değiştirmediğiniz sürece ne yazık ki sunucu işletim sistemi ve sürüm numaraları her sorana bildiriliyor demektir. Botlar internette gezinerek bu bilgileri topluyor ve kötü adamlar bunları kullanıp, zayıf yönlerini bildikleri sunuculara doğrudan hedefli saldırılar gerçekleştirebiliyor. Gösterilen bilgileri kısıtlama yöntemlerini öğrenmek için Google'da hızlıca bir araştırma yapmak yeterli.

20 Modeminizi korumayı unutmayın

İnterneti ne amaçla kullanıyor olursanız olun (evden çalışmak, ticaret veya eğlence) büyük ihtimalle son kullanıcılara yönelik bir kablosuz modem/yönlendirici kullanıyorsunuzdur ve büyük ihtimalle yönlendiriciniz güvenlik açısından bir zayıf nokta durumundadır: Yönlendiriciler genellikle "yükle ve unut" anlayışıyla kullanılırlar ve hiç güncellenmezler. Ne yazık ki bu da onların istismarını kolaylaştırır. Yapabileceğiniz en basit şey, varsayılan ayarları değiştirmek. Yani kullanıcı arabirimine girmek içine kullandığınız kullanıcı adı ve parolasını mutlaka değiştirmeniz gerekiyor. Varsayılan ayarları basit bir Google aramasıyla öğrenmek mümkün.

RouterPasswords.com

Select Router Make: ZYXEL | Find Password

Manufacturer	Model	Protocol	Username	Password
ZYXEL	PRESTIGE	HTTP	n/a	1234
ZYXEL	PRESTIGE	FTP	root	1234
ZYXEL	PRESTIGE	TELNET	(none)	1234
ZYXEL	PRESTIGE 643	CONSOLE	(none)	1234
ZYXEL	PRESTIGE 652HW-31 ADSL ROUTER	HTTP	admin	1234
ZYXEL	PRESTIGE 100IH	CONSOLE	n/a	1234
ZYXEL	PRESTIGE 650	MULTI	1234	1234
ZYXEL	PRESTIGE 900	HTTP	webadmin	1234
ZYXEL	PRESTIGE 645	HTTP	admin	1234
ZYXEL	PRESTIGE P660HW	MULTI	admin	1234
ZYXEL	ZYWALL 2	HTTP	n/a	(none)
ZYXEL	ADSL ROUTERS Rev. ALL ZYNOS FIRMWARES	MULTI	admin	1234
ZYXEL	PRESTIGE 660HW	MULTI	admin	admin
ZYXEL	P-660HW-61 Rev. PRESTIGE 660HW-61	HTTP	n/a	1234

RouterPasswords.com gibi siteler, pek çok yönlendirici modelinin varsayılan parolalarını açıklıyor.

21 Arka kapıları kapatın

Dikkat edilmesi gereken başka bir zayıf nokta daha var: Pek çok modemde, üretim modellerinde geliştirme aşamasında bilerek açık bırakılmış arka kapılar bulunuyor. Saldırganlar bu kapıları kullanıp ağınıza ve bilgisayarınıza sızabilir, verilerinizi ele geçirebilirler. Bu durumda en iyi savunma, cihaz yazılımını güncellemektir: Modem üreticisinin sayfasında bu konuda daha ayrıntılı bilgi bulabilirsiniz.

Ayrıca bazı modemlerde teknik destek için uzaktan erişim olanağı bulunur. Böylece telefonda görüştüğünüz müşteri temsilcisi modem ayarlarınıza ulaşarak onları değiştirebilir. Gerekmedikçe bu özelliği kapalı tutabilirsiniz.

22 SSID'yi gizlemeyin

Kimileri, kullanılabilir ağları tarayan kişiler tarafından görülebilen SSID'nin (kablosuz ağ adı) gizlenmesini tavsiye eder. Ağ adınız varsayılan olarak genellikle modeminizin marka ve modelini içerdiği için riskli olabilir ama tamamen kapatmak da bir hatadır. Bilgisayarınız modeme bağlanırken SSID'niz zaten yayımlanır ve bu bilgi kolayca ele geçirilebilir. Yani ideal çözüm SSID'yi gizlemek değil, varsayılan SSID'yi değiştirmek.

BULUTTA GÜVENLİK

23 Bulut servis sağlayıcınızı seçerken dikkatli olun
Bulut hizmet sağlayıcınızı seçerken dikkatli olun ve sadece fiyattan yola çıkarak tercih yapmayın. Sağlayıcınızın güvenlik denetlemesinden geçip geçmediğini, veri koruma yasalarına uygun olup olmadığını (farklı ülkelerde farklı yasalar geçerli olabileceği için hangi yasalar uygun olduğunu) ve depolanan verilere kimlerin ulaşabileceğini sorgulayın.

24 Verilerinizin tabi olduğu ülkeyi belirleyin
Verilerinizin hangi ülkenin yasalarına tabi olduğuna dikkat edin: Verilerinize kimlerin erişebileceğini belirleyen şey, o muğlak "bulutta" ifadesi değil de, fiziksel olarak depolandıkları konumdur. Avrupa Birliği bu konuda sıkı yasalara sahip olduğu için verilerinizi hem yakınlık hem de güvenlik açısından AB içindeki bir ülkede depolamanızı öneririz.

25 Bulutu şifreleyin
Pek çok hizmet sağlayıcı, verilerinizi şifrelediğinden bahseder. Ama hizmeti satın almadan atmadan önce "şifreleme" derken tam olarak ne kastettiklerini öğrenmeye çalışın. Verileriniz sadece aktarılırken mi şifreleniyor, yoksa depolanırken de şifreli haldeler mi? Bugün hemen hemen tüm bulut depolama hizmetleri dosyalarınızı aktarırken şifreleme uyguluyor ama şifrelenmiş depolama özelliği her hizmette yok. Eğer verileriniz şifrelenerek depolanmıyorsa hizmet sağlayıcınız tüm dosyalarınızı görebilir.

26 Altyapıyı değiştirin
Tercih edebileceğiniz pek çok bulut depolama altyapısı var. Tüm verilerinizi aynı depolama ortamında saklamak doğru olmayabilir. Bir sınıflandırma yaparak verilerinizin değerini belirleyin ve nelerin genel kullanıma açık (bedava veya ucuz) bulutta depolanması gerektiğini, nelerin şifrelenmiş veya kişisel bulutta saklanması gerektiğini belirleyin. Bu konuda genel kural, genel verileri genel bulutta, özel bilgiler içeren verileri ise kişisel bulutta saklamak.

27 Verilerinizin sorumluluğunu üstlenin
Güvenlikle ilgili tüm sorumluluğu hizmet sağlayıcınıza atmayın: Söz konusu olan sizin verileriniz ve siz de gereken özeni göstermelisiniz. Kimin, nelere, ne zaman erişebileceğini belirleyen bir güvenlik politikası oluşturun. Paylaşımlı bir bulut klasöründe, o klasöre artık erişmesi gerekmeyen kişilerin izinlerini hemen kaldırın.

MOBİL KORUMA

28 SMS güvensizliği
Kısa mesajlar da aynen e-postalar gibi kötü amaçlı yazılım yaymak ve dolandırıcılık amacıyla kullanılabilir. Bu nedenle, kısa mesajla telefonunuza gelen linklere dikkatli yaklaşmak gerekir. Mobil kötü amaçlı yazılım dağıtımında amaç artık sadece masaüstü sistemlerinize ulaşmak değil. Suçlular artık telefon rehberinizi ele geçirmek ve ücretli hatları aramak gibi zararlar vermeyi de amaçlıyorlar.

29 Cihazınızı kilitleyin
Mobil cihazlar kolaylıkla kaybedilen ve çalınan cihazlardır. Bu nedenle onları kullanırken özellikle dikkat etmek gerekir. Cihazlarınızı sahipsiz bırakmayın, mutlaka parola koruması ekleyin, SIM kartınıza PIN kodu koyun. Ayrıca uzaktan konum tespiti ve cihazı silme özelliğini de etkinleştirin. "Mobil" dendiğinde akla hemen akıllı telefon ve tabletler gelir ama dizüstü bilgisayarları da unutmamak gerek. Masaüstü bilgisayarlarda karşılaşılan güvenlik sorunlarının tamamı ve daha fazlası dizüstü bilgisayarlarda da karşımıza çıkar, çünkü çalınmaları daha kolaydır. Deneyimli yolcular, dizüstü bilgisayar çantasına benzemeyen çantalar kullanır, hatta yolda uyurken çantanın kayışını kol veya bacaklarına bağlarlar.

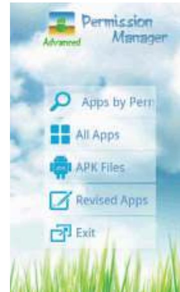
30 Root etmeyin
Sadece yasal uygulama mağazalarından uygulama indirin. Root edilmiş Android veya jailbrake yapılmış iOS cihazları kullanmayın çünkü kötü amaçlı uygulamaların bunlara sızması çok daha kolaydır. İşletim sistemi ve uygulama güncellemelerini de çıkar çıkmaz yükleyin.

31 Uygulamaya sorun
Uygulamaların yüklenmeden önce talep ettikleri izinleri her zaman sorgulayın. İşlevini yerine getirmesi için SMS erişimine ihtiyacı var mı? Eğer yoksa neden talep ediyor? Kötü amaçlı uygulamalar abartılı izinler talep edeceklerdir. Tetikte olmak da fayda var. Bu konuda yardımcı olacak uygulamalar var (örn. Advanced Permission Manager).

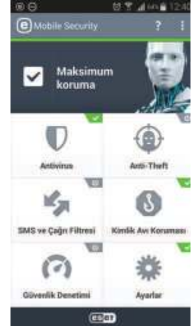
32 VPN kullanın
Mobil cihazınızdan size ait olmayan bir kablosuz ağa (kafe, havalimanı, kütüphane vb.) bağlanıyorsanız verilerinizi şifrelemeniz yerinde olacaktır. Bunun için en ideal yöntem VPN kullanmak. Çok sayıda ücretsiz VPN servisi ve uygulaması var ama bu servislerden sıkça yararlanıyorsanız daha yüksek hız ve güvenlik için beğendiğiniz bir tanesine ücreti abone olmakta fayda var. CyberGhost (cyberghostvpn.com) bizim beğendiklerimiz arasında.

33 Güvenlik uygulaması yükleyin
Mobil güvenlik yazılımları eskisi gibi aldatmacadan ibaret değiller. Eskiden bir güvenlik cilasından başka bir şey sunmuyorlardı ama artık kötü amaçlı yazılımlara karşı savunmanın ilk hattı haline geldiler.

Mobil güvenlik uygulamaları çok önemlidir.



34 Oyunla işi karıştırmayın
Bu maddemiz bilgi işlem departmanı yöneticileri için: Çalışanlarınıza mobil cihazlar veriyorsanız mobil cihaz yönetim teknolojisi kullanın. Bu tür sistemler, sanallaştırma aracılığıyla telefon ve tabletlerde işle oyunun birbirinden ayrılmasını ve ilke temelli kontroller sayesinde personelin güvenlik taleplerini ciddiye almasını sağlarlar. Çalışanlarınız kendi cihazlarını kullanıyorlarsa onları güvenlik konusunda eğiterek ve ağınız üzerinde gereken güvenlik önemlerini alarak daha iyi sonuç alabilirsiniz.



VE SON OLARAK...

Güvenliğin sadece teknolojiden ibaret olmadığını, teknolojiyi kullanan kişilerle de ilgili olduğunu unutmayın.

35 Personelinizi eğitin
En iyi teknolojik savunmalar bile güvenlikten anlamayan personel nedeniyle kolaylıkla aşılabilir. Personel farkındalık eğitimi gereksiz bir lüks değildir. Eğitimin sosyal mühendislik, kötü amaçlı yazılımlar ve güvenli olmayan çalışma yöntemleri gibi en çok karşılaşılan saldırı yollarını ele alması gerekir. Sürekli olarak canlı tutmazsanız üst düzey bir eğitim vermenin hiçbir anlamı yoktur. Bu nedenle sürekli tazeleme dersleri düzenleyin, en son tehditler hakkında güncellemeler yapın. Unutmayın ki amacınız eğitim vermek, utandırmak değil. Bilgisiz çalışanları küçük görmeyin.

ROBOTLAR BİZİ ÖLDÜRECEK Mİ?

Yapay zekanın, insanlığın sonunu getirebileceğini her fırsatta söyleyen Stephen Hawking haklı olabilir mi? İnsanlık belki yakın bir zamanda o meşhur repliği söyleyecek: Ben bir canavar yarattım!

İnsanlardan ölüm sebeplerinin ne olacağını tahmin etmelerini isteseniz muhtemelen alacağınız yanıt kanser veya trafik kazası olur. Bir robot tarafından öldürüleceğini pek kimse aklına getirmiyordur. Mutfak robotunun bir gece kontrolden çıkıp bize saldırmayacağı aşikar. Fakat yapay zeka teknolojisi sürekli gelişiyor ve robotlar tahmin edemeyeceğimiz kadar yoğun biçimde hayatımızda kendine yer edinebilir. Bazı bilimcilere ve teknoloji şirketi yöneticilerine göre bir gün bilgisayarlar insan ırkını ortadan kaldırabilecek kudrete erişebilir. İnsanın kendi yarattığı zeka tarafından alt edilmesi belki bir paranoya fakat ciddiye alanların sayısı hızla artıyor.

Eşyaların ve makinelerin bilimkurgu senaryolarından çıkıp zeki birer ara ırk oluşturarak gündelik hayatımızın parçası haline gelmesine az bir zaman kaldı. Yeni teknolojinin insan varlığına dönük tehdidini ciddiye alan insanlar sadece bir araya gelip kaygılarını gidermekle kalmıyor. İnsanlığın kendi eliyle yok olmasına engel olmak amacıyla Oxford ve Cambridge üniversitelerinden bilimcilerin oluşturduğu bir ekip, yeni teknolojilerin insan varlığına yönelttiği tehdidi öngörmek ve tedbirler almak üzere çalışıyor.

Oxford Üniversitesi çatısında çalışan İnsanlığın Geleceği Enstitüsü (FHI) ile Cambridge Üniversitesi bünyesindeki Varoluşsal Risk Araştırma Merkezi (CSER) kısa süre önce işbirliğine giderek kontrolsüz biçimde farklı alanlarda geliştirilen yapay zeka, robotlar ve nanoteknoloji konularında tehlike senaryoları üzerine çalışıyor. Bu iki kurumdan bilim insanlarının ortak görüşlerinden biri, yaratacağımız yapay sistemin uzun dönem etkilerinin öngörülemeyecek olması.

Cambridge Üniversitesi felsefe profesörü Huw Price'ın öncülüğünde kurulan CSER'ye, en önemli desteği Skype'ın kurucularından Jaan Tallinn veriyor. Yapay zekâ kazasına kurban gitme olasılığının kanserden ya da kalp hastalığından ölme olasılığından daha yüksek olduğunu söyleyen Tallinn'e katılan isimlerden bir başkası da kraliyet gök bilimcisi Lord Martin Rees. Çekirdek kadrosunda felsefeci, yazılımcı ve bilimci barındırması bir fıkra başlangıcı gibi dursa da durum oldukça ciddi.



Akıllı makinelerle ilgili teorilerin başlangıcı esasında çok eskilere dayanıyor. Alan Turing'in Bletchley Park'ta çalışan arkadaşı Irving Good, 1965'te New Scientist'te yayımlanan bir makalesinde, insan tarafından yapılacak bir yapay zekalı makineyle ilgili bazı düşüncelere yer vermişti. Good'a göre bu makine, insanlığın son icadı olacak ve makine kendini üretecek zeka ve yeteneklere kavuştuğunda önü alınamaz bir dönem başlayacak. Yazının genelinde yapay zeka için iyimser tahminlerde bulunan Irving Good, günümüzde yaşıyor olsaydı muhtemelen Stephen Hawking'le pek anlaşamazdı.

KENDİNİ ÜRETEN TEKNOLOJİ

Olumsuz senaryolar çoğunlukla robotların fiziksel ve mental olarak kendi kendilerini üretebileceği bir sürece dayanıyor. Kendi teknolojisini üretene, çoğalan ve kendini her anlamda geliştiren robotların ilk işi insanlardan kurtulmak olabilir ve emin olun bu fikri robotlara bir insan verecektir. Sadece fiziksel olarak değil, duygusal anlamda da insansı robotların yakın gelecekte "piyasaya" çıkmaya başlayacağını görebiliriz. Öğrenen, anlayan, tahmin yürüten, empati kuran, muhakeme yeteneğine sahip robotlar birer dost, yardımcı, sırdaş, hatta sevgili olabilir. İnsana özgü niteliklere sahip robotlar pek çok insanda heyecan uyandırıyor. Distopik senaryosuyla dikkat çeken Black Mirror'ın ilk sezonundaki bir bölümde (Be Right Back) ayrıntılı biçimde anlatılan "robot sevgili" meselesi, sanılandan çok daha derin biçimde insan yaşamını etkileyecek. İnsanla yoğun iletişim halinde olan ve duygusal olarak da hayatında yer edinen yapay zekanın bedeni olmayan haliyle karşımıza çıktığı sinema filmi Her ise görece pozitif bir bakış sunuyor.

Yakın zamanda yapay zekalı robotlar çok daha fazla filme konu olacak ve farklı bakış açılarıyla işlenecek. Robot hakları, yasakları, cezaları ve aklımıza bile getiremediğimiz pek çok ilginç detayı tartışıyor olacağız. Kötü senaryoyu belki daima aklımızın bir köşesinde tutmamız hatta bu konuda tedbiri elden bırakmayan insanları dinlememiz de gerekiyor.



80'lerin ve 90'ların meşhur film serisi Robocob'da yarı insan yarı robot bir polisin hikayesini izledik. Robotlar yakın gelecekte bu kadar iyi niyetli olacak mı göreceğiz

ROBOT GERÇEKLİĞİNİ KABUL ETMELİYİZ

Makinelerin dünyadaki insan varlığını yok etmesinden bahsederken asıl korkulması gerekenler gözle görülenler değil. Nano boyutta robotların sayısız faydası olacağı gibi, ciddi tehditler yaratabileceği de soğuk bir gerçek olarak duruyor. Genetik ve biyoteknoloji alanındaki araştırmalara göz attığımızda, insan varlığının nasıl da pamuk ipliğine bağlı olduğu görülebilir. Kötü amaçlı kullanımda sentetik biyoloji insanlığın sonunu tek başına getirebilecek güçte yaşam formları üretme potansiyeline sahip.

Belki ateşle oynuyoruz, bilmiyorum. Fakat emin olduğum şey, bu konuda yapılacak hataların telafisi olmayacak. Bu yüzden öngörmek zorundayız. Makinelerin vicdan, merhamet gibi insani değerlerden yoksun oluşu, iyi bir amaç için çalıştığını sanarak insanlığa, dünyaya ve tüm canlılara ciddi zararlar vermesine sebep olabilir Küçük bir kod hatasıyla, bir canlı türünün yeryüzünden yok olmasına sebep olabiliriz.

Bu yüzden, kendimizden daha zeki bir tür yaratırken çok dikkatli olmalıyız. Nasıl ki insanlar faydalı bir iş yaptıklarını düşünerek hareket ederken binlerce bitki ve hayvan türünün yok olmasına sebep olduysa ve bunu kendine hak görüyorsa; insan yapımı makinelerin bu yolda gideceğinden emin olabiliriz. Dünyadaki tüm canlıların oluşturduğu ekosistem, insanın bu denli zeki ve yetenekli bir canlı olacağını bilmiyordu, bu konuda hazırlıksızdı. Dünyaya en fazla zararı insanlar veriyor. Benzer bir durum gelecekte makineler için söz konusu olabilir. Bu durumda hazırlıksız olan sadece doğa değil, biz olacağız.

Çözüm bu makineleri ve yapay zekayı geliştirmemek değil. Bu süreci belli kurallar ve standartlara bağlayacak düzenlemeler yapmak, buna uyulmasını iyi biçimde denetlemek. Sürücüsüz otomobil tarafından kaçırılan insan vakaları görmemek için, bugünden bir şeyler yapmaya başlasak iyi olacak. En azından robotlar bizi öldürecek mi dendiğinde aklımıza insanlarla savaşan Terminatör görüntüsü getirmeyelim.



Askeri amaçlarla üretilen robot askerler uzun yıllardan beri cephede etkin biçimde kullanılıyor.

Suçu gerçekleşmeden öngörmek mümkün mü?

Bir suç veya herhangi bir toplumsal olay, gerçekleşmeden çok önce öngörülebilir mi? Kehanetten bahsetmiyorum. Karmaşık algoritmalar, analiz sistemleri, güçlü bilgisayarlar, büyük veri ve yapay zekanın da yardımıyla bilimkurgu filmlerini aratmayan teknolojiler üzerinde çalışılıyor ve sonuç vermeye de başladı diyebiliriz.

Geçen yıl Nextgov adlı güvenlik yayını, bir makale ile Amerikan haber alma teşkilatı CIA bünyesinde kısa süre önce kurulan Dijital İnovasyon Müdürlüğü'nü konu olarak işledi. Sitenin haber kaynağı oldukça sağlam. Kurulan bu birimden sorumlu Başkan Yardımcısı Andrew Hallman. Makalede üzerinden kabaca geçilen mesele, bir süredir hakkında yazmak istediğim bir konu hakkında taze bilgiler içeriyor. Devletler, ileriye dönük isabetli tahminlerde bulunabilecek teknolojiyi geliştirmenin neresindeler?

Sayısal lotodan köşeyi dönmek için pekala kullanılabilecek bu teknolojiler, devletler için kuşkusuz çok farklı anlamlar taşıyor. CIA'in bir alt bölümü olan Dijital İnovasyon Müdürlüğü'nden sorumlu Başkan Yardımcısı Andrew Hallman'ın açıklamasına göre birimleri, ileriye dönük tahmin yeteneğini son bir yıl içinde önemli ölçüde geliştirdi. Çok büyük miktarlardaki veriyi doğru biçimde işleyerek, gelecekte ortaya çıkacak olayları bazen günler, bazense saatler önce isabetli biçimde öngörmek mümkün oluyor. Birbiriyle bağlantısız görünen verilerin yakın gelecekte yaşanacak bir takım olaylar hakkında fikir verdiğini söyleyen Hallman, CIA'in geniş olanaklı veri merkezlerine erişiyor olsalar da, en büyük malzemeyi herkese açık verilerde bulduklarını söylüyor. Yani medyada, yani sosyal medyada, internette.

'TOPLUMSAL OLAYLARI 5 GÜN ÖNCE BİLDİK'

CIA'in üst düzey yetkilisinin en somut ifadelerinden biri, devletlerin teknolojiyi ne denli etkili kullanabildiğine bir kanıt niteliğinde. "Geçmiş dönemde birkaç defa önemli birtakım toplumsal olay ve gerilimleri 5 gün öncesinden öngörebildik" diyen Hallman, özellikle ekonomik krizler ve darbe girişimlerini gerçekleşmeden çok önce görebilmek için yatırımlarını artırdıklarını söylüyor.

Ayrıca Hallman'a göre, devletleri yönetenler artık çok daha şanslı çünkü çok büyük miktarda veriyi farklı biçimde işleyebilen süper bilgisayarlar var ve bu konuda eğitimli analistler bu çıktıları yorumlama konusunda uzman.

GİZLİ SERVİSLERİN GÖZDESİ

Şüphesiz bu konu pek çok devletin ve onlara bağlı gizli servislerin gündeminde. İngiliz istihbarat teşkilatı MI6 için de yıllardır gündemde olan öngörü teknolojisi, sadece toplumsal olaylar için değil, bireysel suçların da yaşanmadan öngörülmesini engellenmesini içeriyor.

Günümüzün aksiyon filmlerine de esin kaynağı olan ajan teknolojileri, son yıllarda büyük ivme kazanan yapay zeka hizmetleriyle daha önemli bir aşama kaydetti. Amerika Birleşik Devletleri'nde üniversitelerle güvenli kurumlarının sıkı sıkıya çalışması da hızlı sonuç almayı etkiledi. 5 yıl önce Los Angeles polisi ike Kaliforniya Üniversitesi (UCLA) arasındaki başlayan işbirliği sayesinde, çete suçlarının işlenmeden önlenmesini sağlayacak bazı tahmin sistemleri geliştirildi. Üniversitede çalışan matematikçiler yakın zamanda, çetelerin nerede ve ne zaman harekete geçebileceğini tahmin edebilen araçlar geliştirdi. Bu araçlar, hangi çetelerin devreye gireceğini bile önceden kestirebiliyor.

Bölgeleri derinlemesine analiz eden ve suç haritalarını detaylı istihbarat bilgileriyle çalışan sistem, hangi çetenin hangi üyelerinin nasıl bir eyleme hazırlandığını matematiksel olarak öngörüyor. Şu ana kadar elde ettikleri sonuçların etkileyici olduğunu söyleyen araştırma koordinatörü Prof. Andrea Bertozzi, kulağa çılgınca gelse de; bu

"Bir suçu işlenmeden öngörüp onu engelleyecek teknoloji günümüzde inşa ediliyor. Gelecekte belki de suç ve kazalar daha yaşanmadan öngörülüp engellenebilecek"



Günümüzün gelişmiş kamera ve video analiz sistemleri sayesinde suçluları anbean izleyen ve davranışlarını yorumlayan yapay zeka, pek çok suçluyu, eyleme geçmeden engelleyecek

analitik programın bilgisayar destekli örüntü tanıma yöntemini kullandığını hatırlatıyor.

Güvenlik birimleri ile üniversitesinin bu ortak projesi, insan etkinliğinin matematiksel modellenmesini içeren çok daha kapsamlı araştırmaların bir parçası. Matematik ve sosyoloji temelli bu karma çalışma, istatistiki verilerde davranış modellerinin tespit edilmesi için deprem bilimi, oyun teorisi ve biyomatematik gibi çalışma alanlarının araştırmalarından faydalanıyor. Ortaya çıkan modellerin dış değerinin hesaplanmasıyla da suç öngörülebiliyor. Ekip, bugüne kadar bu verileri kullanarak çeteler arası şiddet olaylarını ve bölge sahiplenme konusundaki çatışmaları başarıyla tahmin etti. Aynı zamanda suçun işlenme ihtimalinin en yüksek olduğu "sıcak noktaları" da saptamış oldu.

KAMERA SİSTEMLERİ VE SOSYAL MEDYA ETKİSİ

Amerikan polisinin, FBI'ın, CIA'in ve elbette NSA'in elinde onlarca yıllık çok detaylı veritabanları bulunuyor. Tüm bunların birleştirilmesi, süper bilgisayarlar ve yapay zeka destekli yazılımlarla işlenilebilmesi toplumsal hareketliliklerle birlikte özellikle çetelerin işleyeceği suçlara önceden müdahale şansı veriyor.

Bu çalışmalar böyle kalmıyor elbete. Kimi kritik olayları dakikalar önce öngörüp engellemek için, anlık verilere de ihtiyaç duyuluyor. Bu verileri almanın da pek çok yolu var. Şehirlerin neredeyse her sokağında bulunan güvenlik kameraları sisteme taze veri sağlama konusunda benzersiz etkiye sahip. Bir diğer hızlı veri kaynağı da internet, daha doğrusu sosyal medya.

Video analiz yazılımları ve kameralar son yıllarda büyük gelişmek gösterdi. Yüz ev araç tanıma ile kişiler kolaylıkla dışarıda kameradan kameraya izleniyor. Kameralar, belli ortamlardaki olağanüstü hareketlilikleri, aşırılıkları veya sıra dışı durumları hızlıca fark edip merkezi uyarıyor. Belli alanlarda, belli yaş grubunun altına insanların yoğunluk göstermesi de buna küçük bir örnek olabilir.

Diğer önemli araç ise sosyal medya. Toplumsal hareketliliğin nabzı olan sosyal medya, istihbarat teşkilatları için de bulunmaz nimet. Konum bazlı biçimde, belli bir bölgede belirli kelimelerin kullanım sıklığının artması örneğin; işlerin pek de yolunda gitmeyeceğine işaret olabilir.

TARAMA TEKNOLOJİSİNİN KAPSAMI GENİŞLİYOR

Bölgesel bazda yoğunlaşmış suç tahmin sistemlerinin yanı sıra, dünya çapında birçok suçu öngören ve engelleyen organizasyonlar da var. IBM'in desteğiyle geliştirilen Blue CRUSH (Crime Reduction Utilising Statistical History/İstatistiki Kayıtları Kullanarak Suçun Azaltılması) operasyonu da benzer bir örüntü analiz yöntemini kullanıyor. 2005 yılında uygulamaya konan bu proje, sorunlu suç bölgelerini istatistiki bağıntı usulüyle tespit ediyor. Emniyet güçleri de bu veriyi, elindeki imkânları belirlenen bölgelerde değerlendirmek için kullanıyor. Emniyet

yetkilileri, CRUSH operasyonu için pilot bölge seçilen ABD'nin Tennessee eyaletindeki Memphis şehrinde "bu yöntemin uygulandığı bölgelerde suçun mutlak surette azaldığını" öne sürüyor.

Bununla birlikte, ABD Ulusal Güvenlik Bakanlığı (DHS) da suçu işlenmeden öngörmek üzere tasarlanan yeni bir tarama (screening) teknolojisi üzerinde çalışıyor anlatılıyor. Geleceğe Yönelik Tarama Teknolojisi (FAST), istatistiki ve biyolojik verileri değerlendirerek "istenmeyen durumlara dair ipuçlarını" tespit ediyor. Amerikan Bilgi Edinme Yasası kapsamında elde edilen DHS'nin iç yazışmalarından birine göre bu sensörler, "video görüntülerini, ses kayıtlarını ve psikofizyolojik ölçümleri toplamak" için kullanılıyor. Ortaya çıkan veriler de potansiyel faillerin kasıtlarını gerçek zamanlı olarak saptama sürecinde işe yarıyor. Havalimanı gümrük kanalları ve bina giriş noktaları gibi güvenlik gerektiren ortamlarda kullanılmak üzere tasarlanan bu sistem, şu anda gönüllü kamu çalışanları üzerinde test ediliyor.

Bu pilot düzenlemeler, daha başlangıç aşamasında olmalarına rağmen, çok daha genel ve kapsamlı uygulamaları da beraberinde getirebilir. Blue CRUSH operasyonu gibi sistemler, istatistiki verileri analiz ederek davranış örüntülerini inceliyor. Yani bu, doğru veri grubunun işlenmesi sonucunda algoritmaların, ulusal düzeyde veya gündelik yaşamımızda oluşabilecek suç etkinliğini tahmin edebileceği anlamına geliyor.

ETİK SORUNLARI DA BERABERİNSDE GETİRİR Mİ?

Sokaklara güvenlik kameralarının yerleştirildiği tüm ülkelerde kişisel haklar ve mahremiyet tartışmaları yaşandı. Fakat bu gelişen dönemde bu kameraların caydırıcılığı ve suçları çözümlemede oynadığı rol sebebiyle genel bir kabullenme söz konusu oldu. Tüm dünyada devletlerin varandaşını izlediği bir sır değil. Almanya'nın bu konuda eskiye dayanan bir sabıkası var. Ülkesinde yaşayan herkesi türlü yöntemlerle izleyen ve davranış analizi yapan Almanya'nın hemen yakınındaki Estonya'da ise polis, sistemden bir vatandaşın detaylı bilgisine baktığında, o kişiyi bilgilendiriyor ve inceleme sebebini açıklıyor.

Suçu işlenmeden tahmin etmeye yarayan sistemler, her zaman iyi amaçlara hizmet etmeyebilir. Ulus devletler, gizli izleme ve takip teknolojilerini yalnızca suç tespitinde kullanmıyor, aynı zamanda vatandaşlarıyla ilgili yüzlerce terabaytlık bilgiyi başka yöntemlerle topluyor. İnternet şirketleri online faaliyetlerimizi en ince ayrıntısına kadar takip ediyor. Ziyaret ettiğimiz siteleri, kullandığımız uygulamaları, paramızı neye harcadığımızı görebiliyorlar. F-Secure'dan bir güvenlik uzmanı, "Hükümetin kişisel geçmişimize, eylemlerimize, hayatımıza dair diğer detaylara ve özel kayıtlara dayanan ileri düzey tahmin teknolojilerini geliştirmesinin bedeli, harcanacak paranın da ötesinde, kendi özgürlüğümüze kastedilmesidir." diyor ve ekliyor: "Batılı demokrasilerde yaşayan vatandaşların büyük bölümünün, çıkan sonucu gerekçe göstererek bu bedeli ödemeyi kabul ettiğine inanmak gerçekten de mümkün değil."

Etik tartışmalar, genel kesimin mahremiyet endişelerinden ibaret değil. Tahmin ve öngörü sistemlerinin sunacağı sonuçlar daima güvenilir olur mu? Yakın gelecekte hatalı tahminlerin ne gibi bedelleri olur? Hukukçulara göre asıl soru şu: Bu teknolojilerin, hırsızlık ve darp gibi suçlarda çoktan ötekileştirilmiş toplulukları hedef alarak kullanılmasını nasıl engelleyeceğiz?



YENİ DÜNYANIN KARA ŞÖVALYELERİ:

HACKTIVISTLER

Kendilerini modern zaman Robin Hood'ları olarak gören kimi genç hacker'lar, girilmesi zor sistemlere sızma heyecanıyla giriştikleri serüvenin ne gibi ciddi sonuçlarını baştan göremeyebiliyor. Kendilerini "hacktivist" olarak tanımlayan hacker'ların oluşturduğu gruplar, toplumsal ve politik etkileri büyük bazı gelişmelere sebep olabiliyorlar.



HACKTIVISTLER



Son 10 yıldır ivmesini artırarak yükselen hacktivizm hareketinin en önemli oluşumlarından biri şüphesiz Anonymous ve ondan ayrılarak farklı çizgilerde ilerleyen hacker grupları oldu. Ülkesel bazı yapılanmaların bir noktada Anonymous ve ondan ayrılanlar arasında en dikkat çekici grup olan LulzSec'le ortaklaşa giriştikleri siber saldırılar özellikle büyük şirketler ve resmi daireleri hedef alıyor. Elde ettikleri milyonlarca sayfalık belgeleri ve e-posta yazışmalarını uzun süre saklayan ve doğru olduğunu düşündükleri zamanlarda açıklayan hacker'lar, geçtiğimiz yıla kadar internette önemli bir altkültür yaratmayı başardılar.

Geçtiğimiz yıllar içinde Amerika Birleşik Devletleri ve başta İngiltere ve Almanya olmak üzere bazı Avrupa ülkelerinde yürütülen soruşturmalar sonrasında bir dizi tutuklama ve hapis cezasıyla hacker gruplarının üzerlerine gidildi. Yakalanan hacker'ların bir kısmı, hapis yatmamak için gizli servislerle işbirliğine girdi ve gerisi çorap söküğü gibi geldi. Hector Xavier Monsegur olarak hack aleminde nam salan hacktivist'in FBA muhbiri olarak hayatına devam etmesi sonrasında, o ana kadar deşifre olmamış olan James Jeffery, İngiltere'deki evinde uğradığı baskın sonucunda bilgisayarında hack yazılımları çalışır vaziyette suçüstü yakalandı. Hector Xavier Monsegur, LulzSec hareketinin kurucularından biriydi ama 2011 yazında tutuklandıktan sonra muhbir olmuş ve FBI'a her şeyi itiraf ettiği gibi arkadaşlarına da tuzak kurmuştu. En az on ay FBI için çalıştı ve tüm bu süre boyunca Sabu adını kullanmaya devam etti. Onun yardımları olmasaydı Jeffrey ve diğerleri büyük ihtimalle yakalanmayacaktı.

Jeffery, olayı "Polisler kapıyı yerinden söktüler. Tamamen gerçeküstü bir durumdu." Diye anlatıyor. "Yatakta oturmuş Family Guy izliyordum ve hack işleriyle uğraşıyordum. O sırada bilgisayarımı sabit disk olmadan kullanıyordum ve bir şeyleri hack'liyordum. Gürültüden sonra eve hırsız girdiğini düşünmüştüm. Yataktan fırlayıp merdivenlerden aşağı doğru koşunca polislerin şok tabancalarını bana doğrulttuklarını gördüm. Gelenlerin polis olduğunu tahmin etmediğim için bilgisayarın fişini çekmeyi de akıl edemedim. Bu yüzden de tüm programlar bilgisayarımda açık bir şekilde yakalandım." şeklinde anlatıyordu. Birkaç gün sonra, Asperger sendromu olan Jeffery kendisini Wandsworth Hapishanesi'nde buldu. Geride bıraktığı delilleri silmesini ve başka hedeflere yönelmesini engellemek için kefaletle serbest bırakılma talebi reddedildi. Duruşmalarda



yaptıklarından ötürü çok pişman olduğunu söyleyen Jeffery, bu davranışlarını yaşadığı depresyon ve alkol sorunuyla savunmuştu.

Pişmanlık duyan veya büyük kurumlardan çalınıp internette yayımlanan verilerin sıradan insanlara daha fazla zarar verdiğini fark eden tek eski hacktivist o değil. Eski LulzSec üyesi Ryan Cleary, bir etkinlikteki konuşmasında "Saldırdığım kurumlar için değil ama bu saldırıların masum insanlara, parolaları internete sızdırılan insanlara verdiği zararlardan dolayı duyduğum bir pişmanlık var." demiş ve sözlerine şöyle devam etmişti: "Bu insanlar, kişisel verilerini, son derece kötü güvenliğe sahip olan şirketlere emanet etmişlerdi. Bu şirketler saldırıya uğrayınca, bu kişilerin bilgileri sızdırıldı ve dolayısıyla şirketten daha fazla zarar gördüler. Onlar için ve hesaplarının istismar edilmesinden dolayı üzülmemiz normal."

Ancak saldırılar sırasında kişisel motivasyon, bu tür kaygıları hissetmenin önüne geçiyordu. Hacker'ların arasında "Amerika'daki bir siteyi çökerttim" gibi ifadelerle eylemlerini başkalarına duyurmak oldukça güzel bir duygu. Basının ilgisini de çektiklerinde gerçek bir adrenalin patlaması oluyor. Hacker'ların büyük bölümü politik görüşlerinden veya politik sebeplerden ötürü saldırı hedeflerini büyütüyor ve özellikle devlet kurumlarına ve siyasetçilere yöneliyor. Çünkü asıl heyecan orada başlıyor.

"HACK DE BİR PROTESTO TÜRÜ"

Özellikle Anonymous ile LulzSec

Bazı hacker grupları kendilerini "modern çağın Robin Hood'ları" olarak tanımlıyor.

gruplarının yaptığı bazı küresel "operasyon"ları hack faaliyeti olarak sınıflandırmak haksızlık olur. Tunus ve Zimbabve gibi bazı ülkelerde, insanların Facebook ve Twitter'a takip edilmeden girmelerini sağlamak için kod yazmış olmaları unutulmamalı. Hüküm giymiş diğer dört eski LulzSec üyesi, buna benzer faaliyetlerini örnek göstererek, kendilerini modern çağın Robin Hood'ları olarak tanıtıyor ve niyetlerinin "iyi şeyler" yapmak olduğunun altını çiziyor. Bu yaptıklarının hackleme olmadığını ve yasa dışı bir yanı bulunmadığını söyleyen LulzSec üyeleri, yaptıkları siber salıdırıları ise "gerçek dünyadaki gösteriler gibi meşru bir protesto biçimi" olarak savunuyor. Bu anlamda, LulzSec grubunun hack eylemlerinde oynadığı rolden dolayı tutuklandığında 16 yaşında olan Mustafa Al-Bassam şu sözleri kayda değer: "Bana sorarsanız, eğer DDoS saldırısı düzenleyen bilgisayarlar botnet'lerin değil de gönüllü kullanıcıların kontrolündeyse gerçek bir oturma eylemiyle bunun arasında bir fark yoktur."



HACKER'LIKTAN IŞİD'E UZANAN YOL

Yetkililer bu konuda farklı düşünüyorlar ve hack konusunda katı bir tutum takınıp bu faaliyetlere katılanları cezalandırarak potansiyel hacktivistleri caydırmaya çalışıyorlar. Hacker'lar devlet kurumlarını ve dev firmaları hedef almaya başlayınca kurulu düzen de işi ciddiye almaya başladı.

LulzSec Dörtlüsü'nün aldığı ceza açıklanırken başsavcılıktan Andrew Hadik şunları söylemişti: "Yol açtıkları zarar öngörülebilir, kapsamlı ve kastiydi. Yüz binlerce masum insanın hayatlarına ilişkin özel ayrıntıları ele geçirip yayımlayacaklardı. Firmalar da ciddi finansal zararlarla karşılaştılar, itibarları zarar gördü. Bütün bunların aslında eğlenceli olduğu söylersek, yaptıklarının ciddiyetine gölge düşürmüş oluruz. Aslında son derece ciddi suçlar işliyorlardı."

Örneğin TeaMpoisoN grubunun üyelerinden, internette Trick adıyla tanınan Junaid Hussain, 2012 yılında Tony Blair'e ait kişisel bilgileri sızdırmak ve İngiliz terör ihbar hattını "telefon bombardımanına" tutarak işlemez hale getirmek suçlarında oynadığı rolden dolayı altı ay hapis cezasına çarptırılmıştı. Cezaevinden çıktıktan sonra tekrar hack faaliyetlerine bulaşan Junaid Hussain, Suriye'ye giderek IŞİD'e katıldı. Kısa sürede örgüt içine en üst kademelere yükselen ve IŞİD'in "siber istihbaratçısı" olarak bilinen Hussain'in, 25 Ağustos 2015'te bir drone saldırısı sonucu öldürüldüğü biliniyor.

Amerikalı bir gazeteci olan Sean Sullivan, ölümünden kısa süre önce Junaid Hussain'le Twitter üzerinden yazıştığını iddia etmiş ve şunları yazmıştı: "Onun inanacak, bağlanacak bir şeyler arayan bir çocuk olduğunu görmek zor değildi. Tam anlamıyla, uğruna mücadele edeceği bir şeyler arayan bir asiydi. Trick şimdi Suriye'de. O, hukuka karşı geldikten sonra İngiltere'de bir geleceği olmadığını düşünüp Suriye'ye giden gençlerden biri. Zeki birine benziyordu. Aktivist hacker'lara, daha sonra yasal bir işle uğraşmaları imkânsız hale gelecekmiş gibi davranmamız çok yazık."

YAKALANANLARIN ÇOĞU HAPİS CEZASI ALDI

Başta LulzSec ve Anonymous üyeleri olmak üzere pek çok hacker, yakalandı ve uzun duruşmalardan sonra ağır cezalara

Ceza alan hacker'lar, hapisten çıktıktan sonra kötü sicilleri sebebiyle iş bulmakta zorlanıyor ve kendilerini yeniden yasadışı faaliyette buluyor

çarptırıldı. Bu yakalanmalarda teknik takipten ziyade, grup içinde yaşanan ihanetlerin ve ele vermelerin büyük payı var.

LulzSec üyesi Ryan Cleary (Viral), yakalandıktan sonra CIA ve Pentagon sitelerini hack'lediğini itiraf etti. İki yıl sekiz ay cezaya mahkum oldu. Esker Ryan Ackroyd (Kayla), 24 yaşındayken yakalandı. Sony'ye ve başka büyük şirketlere saldırmaktan 2,5 yıl hapis yattı. LulzSec'in sözcüsü olan Jake Davis, 18 yaşında tutuklandı ve iki yıl hapis yattı. Bir başka LulzSec üyesi olan Mustafa Al-Bassam (Tflow) ise 16 yaşındayken yakalanarak tutuklandı. Programlama dehası olarak görülen Al-Bassam, bir yıl sekiz ay hapis cezasına çarptırıldı.

Cezaya çarptırılmış hacker'ların ihanet, stres, hapishane ve suç geçmişinden kaynaklanan sorunlardan dolayı hayal kırıklığına uğrayıp kenara çekildiklerini düşünebilirsiniz. Ancak 32 ay hapis yatan James Jeffery gibi pek çok hacker, içeride olmanın en büyük eksikliğini "Anonymous faaliyetlerinden uzak kalmak" olarak açıklıyor.

Eski hacker James Jeffery'e ulaşıp yeteneklerini ne olduğu belirsiz işlerde kullanmasını isteyen kişiler olmuş ama henüz tam zamanlı bir iş bulabilmiş değil. "Birkaç iş başvurusunda bulundum. Hepsinden ret cevabı aldım. Sebep genellikle sabıkam olmasıydı. Sabıka kaydı iş bulmaya çalışırken pek bir işe yaramıyor". Bunun yerine kendi geliştirdiği birkaç web tabanlı proje üzerinde çalışıyor. Arada sırada da hem Google hem de Facebook'un güvenlik açıklarını tespit edenlere ödül verdiği programlar aracılığıyla para kazanıyor.





Kalabalık Mekanlar için Akıllı Güvenlik ve Hızlı Analiz

Hastane, AVM, okul, havalimanı, otel ve fuar alanı gibi halka açık kalabalık mekanların takibi, Sensormatic'in çözüm portföyüne eklediği yeni video analiz çözümü Avigilon Appearance Search ile farklı bir boyut kazanıyor.

Güvenlik kameralarını çok daha işlevsel hale getiren ve güvenlikte yeni bir vizyon ortaya koyan bu çözüm, görüntüler içinde tespit edilen unsurlar hakkında, geriye dönük otomatik arama yapmaya imkan sağlayarak, güvenlik birimlerine de çok hızlı biçimde sonuca ulaşma avantajı kazandırıyor.

Yoğun insan sirkülasyonunun olduğu alanların güvenliği ve takibi her zaman daha kritik önem taşır. Günümüzde etkili yöntemlerden biri olan güvenlik kamerasıyla takip, yeni video analiz teknolojileri sayesinde şekil değiştirdi. Lider elektronik güvenlik entegratörü Sensormatic'in müşterilerine sunduğu yeni çözümlerinden biri olan Avigilon Appearance Search (Detaylı Takip Analizi), saatlerce uzunluktaki kayıtlı veri üzerinde çalışarak istenen sonuca dakikalar içinde ulaşmayı mümkün kılıyor.

Arama motoru gibi çalışan sistem, görüntüde seçilen belirli özellikteki bir cismin veya kişinin görünüşünü baz alarak o alan içindeki tüm kamera görüntülerini tarıyor ve değişiklik geçmişine ulaşıyor.

FARKLI KAMERA GÖRÜNTÜLERİNDE ARAMA YAPMAK MÜMKÜN

Örneğin, havaalanı koridorunda tespit edilen sahipsiz bir çantanın, oraya kim tarafından ne zaman bırakıldığının tespiti için önce ilgili çanta ekranda seçiliyor, sonra da kamera görüntüleri içinde arama yapılıyor. Bu örnekte, seçilen obje yani sahipsiz çantanın, mekanda kullanılan tüm kameraların kayıtları içinde aranması da mümkün oluyor. Geçmiş zaman dilimi içinde çantayı oraya bırakan kişi tespit edildikten sonra o kişinin görüntüsü sisteme tanımlanıyor ve şahsın, farklı alanlarda konumlandırılmış diğer kameraların görüntüleri içinde de tespiti sağlanıyor.

Bugüne kadar kullanılan video analiz sisteminde seçilen nesnenin, yani örnekteki çantanın oraya ne zaman bırakıldığı görülebiliyordu. Bu çözüm sayesinde aynı alandaki farklı kameraların aldığı görüntüler içinde arama yapılabiliyor ve çantayı bırakan kişinin nereden geldiği, ne zaman bıraktığı ve sonrasında nereye gittiği anbean izlenebiliyor.

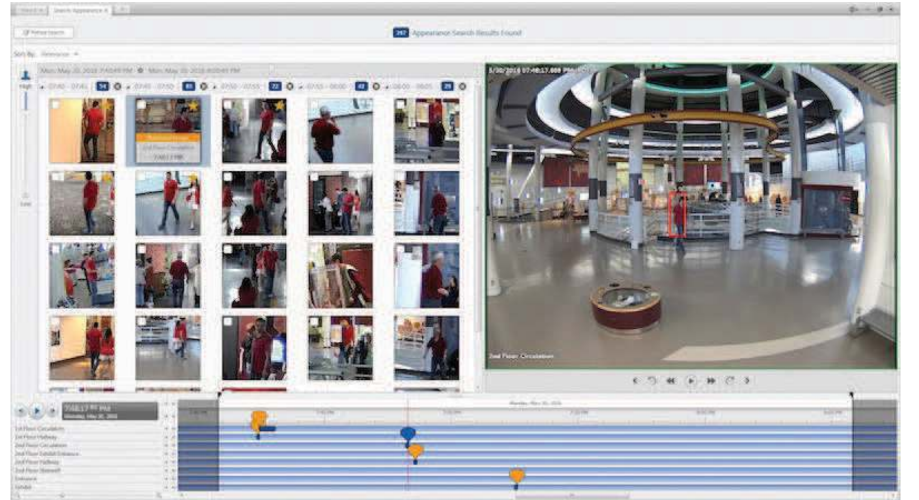
SAATLERCE UZUNLUKTAKİ GÖRÜNTÜ BİRKAÇ DAKİKADA TARANIYOR

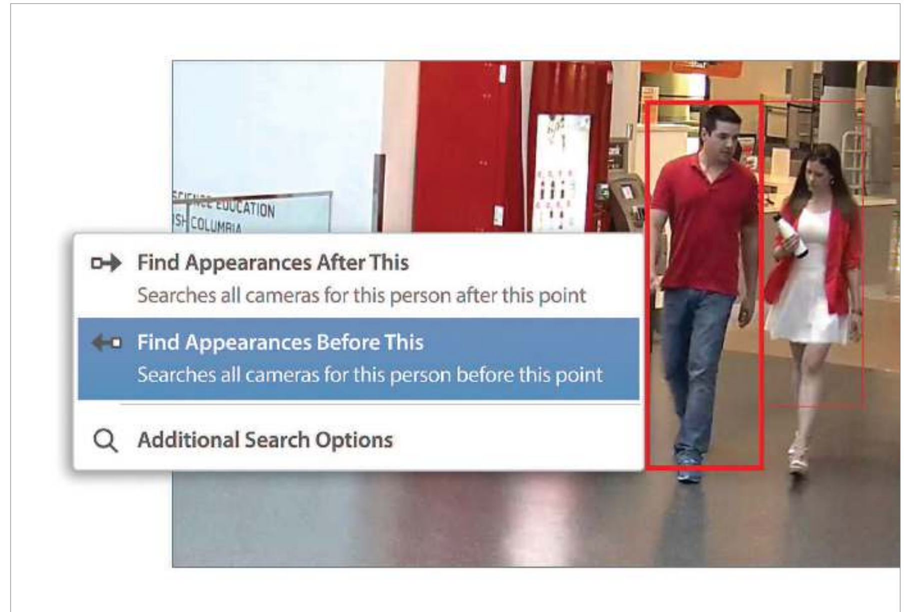
Güvenliğin büyük önem taşıdığı okul, havalimanları, alışveriş merkezi, hastane ve otel gibi kalabalık mekanlarda şüpheli durumlarla ilgili hızlı analiz ve sonuca çabuk ulaşmak hayati önem taşıyor. Sensormatic'in bu yeni çözümü sayesinde geriye dönük kamera kayıtları içinde yapılan arama ile şüpheli duruma ve şahsa çok daha kısa sürede ulaşmak mümkün oluyor. Adli delil olarak da kullanılabilen bu görüntülerin, alandaki tüm kameraların çektiği saatlerce uzunluktaki kayıtlar içinden tespit edilmesi ise birkaç dakikada sağlanabiliyor.

SENSORMATİC'LE GÜVENLİKTE YENİ BİR VİZYON

Sensormatic CEO'su İsmail Uzelli, "İnsan hayatına dokunan, pratik faydalar sağlayan çözümler geliştiriyoruz. Appearance Search bu çözümlerin en güncel örneklerinden biri. Dünyanın önde gelen Video İzleme Teknolojileri markası Avigilon tarafından geliştirilen bu video analiz sistemi, günlük hayatta da önemli katkılar sunacak. Örneğin alışveriş merkezinde ansızın kaybolan bir çocuğun nerede olduğunun, tüm kameralardan elde edilen görüntüleri tarayarak, dakikalar içinde bulunabilmesi bir devrim. Benzer örnekler çoğaltılabilir. Özetle söyleyebilirim ki; Sensormatic olarak sunduğumuz bu çözüm, yepyeni bir güvenlik vizyonu ortaya koyuyor." dedi.

Akıllı kameralar ve elde edilen görüntüyü çok hızlı biçimde işleyen yapay zekalı bilgisayarlar sayesinde güvenlik yepyeni bir anlam kazanıyor





RADARLAR GÜVENLİĞİN HİZMETİNDE

Radyo dalgaları ile bölgeyi tarayarak, objelerin hızını, yönünü ve yerini belirleyen radarlar güvenlik sektöründe de kullanılmaya başlıyor.





Radarlı güvenlik çözümleri, çevrelerindeki objeleri araç ya da insan olarak detaylı tanımlayarak tehditleri anında tespit edebiliyor, ayrıştırma özellikleri sayesinde ise hayvan girişi gibi yanlış alarmları engelliyor.

Özellikle havalimanları, büyük siteler, ticari tesisler gibi geniş alanların güvenliği için önerilen radar sistemleri, hızlı kurulumun yanı sıra, yıllık bakım, kalibrasyon gibi teknik gerekliliklerin az olması nedeniyle maliyet avantajı da sunuyor. Radar sistemleri, karlı ve sisli gibi kamera görüşünün zorlandığı ağır hava koşullarından etkilenmiyor.

TEHLİKE UZAKTAYKEN FARK EDİLİYOR

Radarlar bugüne kadar en çok savunma sanayi, trafik, meteoroloji ve havacılık sektöründe karşımıza çıkıyordu. Güvenlik kapsamının genişlemesi, radar üreticilerinin güvenlik uygulamalarına uygun ürünler üretmesi ve fiyatlarının son kullanıcı için ulaşılabilir hale gelmesi sayesinde radar sistemleri standart çevre güvenlik bileşenlerinden biri haline geldi. Artık özel mülkler, havalimanları, veri merkezleri ve sınır bölgelerinde radar ile tehlike uzaktayken fark edilecek.

GÜVENLİKTE ZAAFİYET BIRAKMIYOR

Standart çevre güvenlik uygulamalarında; tel-çit üzerine yerleştirilen kablolarla çevrili alana izinsiz giriş tespit edilir, ardından tehdit hareketli kameralarla takip edilerek aksiyon alınması sağlanır. Radar yazılımlarının; video izleme, tel-çit algılama gibi farklı güvenlik sistemleriyle aynı dili konuşabilmeleri sayesinde herhangi bir tehlike durumunda objenin hareketli kameralar tarafından otomatik takibi ve hızlı aksiyon alınabilmesi mümkün oluyor. Radar

> Radarların güvenlik amaçlı kullanım alanları gün geçtikçe çeşitleniyor ve çok daha kesin çözümler sağlıyor



sistemlerinin de bu tip uygulamalara dahil olması sayesinde artık tehlikeler tel-çit noktasına ulaşmadan algılanıp çok daha erken aksiyon alınması sağlanabilecek.

MALİYET AVANTAJI VE KURULUM KOLAYLIĞI

Kurulum kolaylığı ve maliyet avantajı sayesinde güvenlikte giderek daha fazla kullanılması beklenen radarlar, uzun zamandır güvenlik sektörünün ilgisini çekiyordu. Ancak yüksek maliyetler, kullanılması önündeki en büyük engeldi. Diğer teknolojilerde olduğu gibi radar teknolojisindeki gelişmeler de maliyetleri ulaşılabilir hale getirdi. Radarların yakın gelecekte güvenlik sistemlerinin vazgeçilmez bir bileşeni olacağından şüphe yok.



Şirketler Alışverişlerimizi Nasıl Takip Ediyor?

Şirketler alışverişlerimizi nasıl takip ediyor? Bu bilgiyle ne yapıyorlar ve bu bizim için sorun mu? Yanıtı bulmak için alışverişe çıkıyoruz.

Yerel süpermarketten ya da internetten ne zaman alışveriş yapsak izleniyoruz. Ne zaman kasada para ödesek ya da bir internet mağazasında gezinsek, bu dijital ormanda ekmek kırıntılarından bir iz bırakıyoruz ve bu iz satın alma alışkanlıklarımıza, kişisel bilgilerimize uzanıyor. Şirketler işte bu izi sürerek ilgi alanlarımızı ve satın aldıklarımızı kapsayan profiller oluşturuyor. Peki, toplanan bu verilere ne oluyor? Mademki böylece bir sürü bilgi topluyorlar, kişiye özel teklifler neden hep isabetsiz?

Bugünlerde satın alma alışkanlıklarımızın şöyle ya da böyle kayıt altında olduğunun siz de farkındasınızdır. Kasada ödeme yaparken o mağazaya ait müşteri kartını uzattığınızda, aslında gelecekte satın alacağımız ürünlerden indirim sağlayacak puanlarımızı artırıyor ve karşılığında mahrem alanımızdan biraz daha vazgeçiyoruz. Benzer şekilde, internetten alışveriş yaparken de kredi kartı bilgisi, e-posta adresi gibi kişisel bilgilerimizi çevrimiçi satıcıya teslim ediyor, karşılığında bize cazip tekliflerle (ücretsiz kargo, indirim kuponu, hediye çeki vb.) gelip bizi tekrar mağazalarına çekmelerine izin veriyoruz.

Peki, hakkımızda tam olarak hangi verilerin toplandığını, nasıl işlendiğini ya da satıcıların bu bilgiyi ilerde ne yapmayı düşündüğünü biliyor muyuz? Muhtemelen yanıt hayır ve çok da endişe etmiyorsak bunun sebebi, satıcıların veriyi kullanmada pek de becerikli olmamaları. Hâlâ satın almayı hayatta aklımızdan geçirmeyeceğimiz şeylerin, ağzımıza bile koymayacağımız yiyeceklerin reklamlarını alıyoruz.

Peki, bunca veriye rağmen neden satıcılar neyi sevip neyi sevmediğimizi öğrenemiyor? ▶



Marks & Spencer'ın Türkiye'de müşteri kartı uygulaması var, İngiltere'de ise müşteri avantajları eklenmiş kendi kredi kartını sunuyor.



APT, Starbucks gibi firmalar için müşteri verilerini analiz ediyor.



Vivian Braun şirketlerin müşteri kredi kartı numaralarından yola çıkarak tüketici davranışlarını analiz edebileceğini söylüyor.

Bunu anlamak için verinin nasıl toplanıp işlendiğine bakmamız gerekiyor.

Hedefe kilitlenmek

William Weidman dünyanın en büyük satıcılarıyla alışveriş alışkanlığımızı daha iyi takip ve tahmin etmek için çalışan APT (Applied Predictive Technologies) firmasının başkan yardımcısı. APT'nin birlikte çalıştığı firmalar arasında Asda, Barns & Noble, Starbucks ve Staples gibi büyük isimler var. Weidman, bir dükkâna gittiğimizde yaşananları ve nelerin takip edildiğini şöyle örnekliyor: "Kredi kartı ya da müşteri kartı sayesinde elimizde bir 'müşteri tanımlayıcısı' oluyor ama o kişinin kim olduğunu henüz bilmiyoruz." diyor. "Bununla birlikte müşterinin dükkâna şu anda gelip beş ürün aldığını biliyoruz. Dört hafta sonra tekrar gelip üç parça ürün aldığını da. O zaman elimizdeki birincil veri kümesi bu. Satın alınanlar, hangi ürünlerin birlikte alındığı ve bunları hangi müşterinin aldığı."

Birçok kişi sadece müşteri kartıyla (sadakat kartı) yapılan alışverişlerin takip edildiğini düşünüyor ama durum öyle değil. "Müşteri kartı kullanmadan da birçok şeyi öğrenmek mümkün." diyor IBM'in satıcılarla ilgilenen iş analiz müdürü. "Bir kişiyi takip etmek istiyorsanız, alışveriş alışkanlıklarını örneğin kredi kartından da takip etmek mümkün. Bu onlar hakkında çok fazla şeyi ele veriyor."

Müşteri kartıyla yapılan alışverişlerin farkı, satıcının bu bilgiyi müşteriyi temsil eden anlamsız bir rakamla değil de müşterinin kim olduğuyla ilişkilendirebilmesi. Bu da zaman içinde alışverişlerimizin daha kolay takip edilmesini sağlıyor.

Bu türden bir izleme masum görünüyor olabilir ama zaman içinde satıcılar hakkımızda çok ayrıntılı profiller çıkarabiliyor. Örneğin bir mağaza, sizin 45-50 yaşlarında, iki kedisiyle yaşayan bir kadın olduğunuzu, oğlunuzun ya da kızınızın yakında doğum yaptığını ve 50 kilometre uzakta oturduğunu anlayabiliyor. Bu kadar isabetli bir profili nasıl mı oluşturuyor? Çünkü müşteri kartı



William Wiedman şirketlerin alışveriş davranışlarımız hakkında milyarlarca veri kümesi kaydettiğini belirtiyor.

almak için doldurduğunuz form sayesinde zaten adınızı, yaşınızı ve cinsiyetinizi biliyor. Satın aldığınız kedi mamasının miktarından evinizde kaç hayvan olduğunu, yiyecek alışverişlerinizden de yalnız yaşadığınızı anlıyor. Hatta sizin uzaktaki bir şubeden sürekli bebek malzemesi almanızdan yola çıkarak, kızınızın ya da oğlunuzun yeni çocukları olduğu sonucuna varabiliyor.

İz peşinde

Satıcıların bu verinin peşinde olmasının birçok nedeni var. Hafta sonu gazetenizin içinden çıkan eklerde hangi kampanyaların olacağını, raflara hangi ürünlerin yakın dizileceğini bu sayede belirliyorlar. O yüzden, hazır İtalyan yemeği yemek istediğinizde bir şişe Chianti ve biraz sarımsaklı ekmek el altında oluyor. Bu veriyle yeni şubelerini nerede açacaklarını belirliyor, hatta bazen hepsini size kendi ürünlerini pazarlamak isteyen başka şubelere satıyorlar.

Kulağa çok korkunç geliyor ama toplanan bilgi sızdırılırsa ya da doğru dürüst korunmazsa tehlikeli olabilir. Örneğin 2006'da AOL arama verilerini sızdırılması, sözde isim bilgileri silinerek anonimleştirilmiş verilerin bile birleştirilip sahibinin bulunabileceğini gösterdi. New

Sadakat kartlarının değeri

Müşteri kartı da denilen sadakat kartları (loyalty card), onlarca yıldır tüm dünyada kullanılıyor. Sadakat kartları, adından da anlaşılacağı üzere, müşterilerin belli bir markaya olan sadakatleri (sürekli o mağazadan alışveriş yapmaları) karşılığında müşteriye bazı avantajlar sağlayarak marka bağlılığını teşvik ediyor. Ancak son akademik araştırmalar bu kartların sadakati sağlamada çok az etkili olduğunu gösteriyor.

Aslına bakılırsa müşterilerin bu kartları talep etmelerinin sebeplerinden biri, zaten o markaya sadık olmaları. Çoğu ülkede sadakat kartlarının ödülleri oldukça düşük ve genelde toplam alışveriş miktarının yüzde biri kadar indirim sağlıyorlar.

Sadakat kartlarının firma için değeri tüketici için olandan çok daha yüksek, çünkü kartlar sayesinde topladıkları bilgilerle müşterilerini yakından tanımakla kalmıyor, bu bilgileri üçüncü şahıslara da satarak ek gelir elde edebiliyorlar. Gizlilik taraftarları tarafından sürekli topa tutulsa da bu uygulama ne yazık ki oldukça yaygın.



York Times, 4417749 numaralı müşterinin, sırf yaptığı aramalardan yola çıkarak Georgia'da yaşayan 62 yaşındaki dul Thelma Arnold olduğunu buldu (ve kendisinden izin alarak açıkladı). Doğal olarak veri izlemeye yönelik büyük bir mahremiyet hareketi başlatıldı ve verilerin daha fazla anonimleştirilmesinden şirketlerin müşteri hareketlerini takibinin yasaklanmasına kadar birçok talepte bulunuldu.

Ancak veri toplamanın kötülüklerini duydukça, elde edilen verinin gerçekte satıcılar tarafından ne kadar isabetli kullanıldığıyla ilgili soru işaretleri oluşuyor. Biz müşteriler için veri izleme her zaman kötü bir şey değil. Bazen bir sitenin hoşumuza gidecek yeni filmleri, okumadığımız ama sevebileceğimiz kitapları önermesini, hep kullandığımız temizlik malzemesinin daha ucuz alternatifini göstermesini isteyebiliriz. Ne yazık ki şirketler bu konuda, veri toplamaya başlamadan önceki hallerinden çok da ileri gidememiş görünüyor.

Hakkımızda herkesten çok şey bilen Google bile reklam verenleri hedefe yönelik reklamların faydaları konusunda ikna etmekte zorlanıyor. En son rakamlar, arama yaptığınızda karşınıza çıkan AdSense reklamları için reklamcıların tıklama başına giderek daha az ödeme yaptığını gösteriyor. Hedefli reklamcılık konusunda AdSense en hızlı, en basit ve en doğrudan örnek; çünkü sizin arama kutusuna yazdıklarınız doğrultusunda belirleniyor.

Hedefi ıskalarken

Peki, o zaman veri toplamadaki patlamaya karşılık neden daha isabetli, daha yararlı indirimler, teklifler ve kuponlar almıyoruz? Bunun bir nedeni, şirketlerin şu anki müşteri takip düzeyi kapasitesinin, işleyemeyecekleri kadar çok veri toplaması.

APT'den Weidman, şirketlerin verileri hangi sıklıkta kaydettiği sorulunca, "Her zaman, her şeyi kaydediyorlar." diye yanıtlıyor. "Çok büyük şirketler için milyarlarca veri kümesinden söz ediyoruz. Bu kadar çok verinin izini sürebilmek bundan birkaç yıl önce mümkün hale geldi. Daha fazla satıcı ayrıntılı takibe başlayınca, tüm bu veriyi anlamlı sonuçlar elde edecek şekilde işleme sorunu çıktı."

Veriyi sırf kaydetmiş olmak için kaydetmemek, bundan bir şeyler çıkarmak işin zor yanı. Verinin miktarı da büyük bir sorun ama başka faktörler de var. "Şirketler ve bu tür verileri kaydeden organizasyonlar anlamlı sonuçlara ulaşıp müşterileri için kişiselleştirilmiş bir deneyime dönüştürmek için var güçleriyle çabalıyorlar." diyor SAP Müşteri İlişkileri Yönetimi Müdürü Kris McKenzie.

Şirket en büyük satıcılarla, ürünlerin raflara konuşundan satın aldıklarımızın kasada toplanmasına kadar birçok konuda işbirliği yapıyor.

"Veri hacmi bir sorun ama verinin dağınıklığı da önemli." diyor McKenzie. "Genellikle bu veriler tek bir yerde değil, birden çok veri sistemine yayılmış durumda oluyor. O yüzden, çoğu satıcının pazarlama için birçok kanalı var ve her kanal aslında bir depo."

Bu yüzden de örneğin paralı TV yayını yapan bir şirketi aradığımızda çağrı merkezi genelde web sitesinden satışın yapıldığı sistemden ayrı bir sistem üstünde çalışıyor. Eğer telefonda sizin için uygun yayın paketini belirleyip alışverişinizi web sitesinden tamamlamak isterseniz karşınıza farklı fiyat çıkabiliyor çünkü sistemler birbirinden bağımsız çalışıyor.

"Eğer çağrı merkezini ararsanız, sizin web sitesinden alışveriş yapmakta olduğunuz şahıs olduğunu anlamaları çok güç." diyor McKenzie. "Farklı sistemlerde, farklı süreçlerden geçen ve farklı veri tabanlarında tutulan bu iki bilgiyi nasıl bir araya getireceksiniz?"

IBM'den Braun, alışveriş yöntemlerimizdeki artışın müşterilerle başa çıkmayı güçleştirdiğini söylüyor. "Bence şu an satıcılar için en önemli sorun, satış kanallarının çoğalması." diyor. "Müşteriler onlara farklı yollardan geliyor: cep telefonu, internet ve mağaza. Müşterilerine tutarlı, bir bütün oluşturan, memnuniyet verici alışveriş deneyimi yaşatmaya çalışıyorlar fakat müşteri araştırmasını internetten yapar, ertesi gün dükkâna gider, sonra tekrar internetten sipariş verirse bununla başa çıkmak güç."

Ana hatlar

Bir başka sorun da belli müşterilere odaklanmanın pratik olmayışı. Onun yerine satıcılar bizi geniş ve genelde



İngiltere'nin en büyük sadakat kartı ağı Nectar'ın desteklediği markalar arasında Apple, Dell, eBay, Ford gibi devler de var.



Müşteri izleme sürekli iyiye gidiyor olabilir ama kişiselleştirilmiş indirimler hâlâ gelişigüzel görünüyor.

isabetsiz profil kategorilerine sokup verileri böyle analiz ediyor. "Bu verilerin birçoğu gruplara ayırmanın sonucu." diyor APT'den Weidman. "Gruplama ise alışveriş profilinize göre yapılıyor: mağazaya gelme sıklığınız, alışverişte sepetinizin büyüklüğü, satın aldığınız mal türleri…"

Daha güncel sistemlere sahip olanların daha kişisel tekliflerde bulunabildiğini söylüyor Weidman. "Kimileriyse 'X ürününü aldığınız için Y ürününün onun yanında iyi gideceğini düşünüyor ve size Y ürününde özel indirim sunuyoruz.' diyebilecekleri bireysel müşteri düzeyine inebiliyor." Ancak kimi zaman buna satıcıların geri kafalılığı engel oluyor. Biz müşterilerin kampanya ve indirim olarak ne istediğine değil de, belli ürünlere aşırı odaklanıyorlar.

"Müşteri perspektifinden bakıldığında, sevildiğinizi, önemsendiğinizi ve satıcının sizi tanıdığını bilmek istiyorsunuz." diyor Braun. "Ama bir yandan da satıcının sizi gereksiz ya da aşırı fazla teklife boğmamasını istiyorsunuz. Sorun şu ki satıcılar genelde hepsini birden yapmaya kalkışıyor. 'Harika bir kampanya hazırladık!' deyip ellerindeki 20 milyon e-posta adresine birden yolluyorlar."

Paul Alexander, sahipleri arasında Visa Europe'un da bulunduğu ve satıcılara kaydettikleri müşteri verilerinden anlam çıkarmada yardımcı olan Beyond Analysis firmasının CEO'su. Birçok şirketin veriyi doğru düzgün işleyip müşteriyle temasa geçmeden önce anlamak yerine, ürünleri insanlara ulaştırmaya odaklandığını belirtiyor.

"Benim için bu kopukluk çok temel bir sorun ve nereye baksak görüyoruz." diyor. "Verileri kaydediyorsam ne anlama geldiklerini ya da tüketici davranışını anlıyorum mantığı bu. Sırf bir e-posta pazarlama veri tabanına kayıtlı müşterileri var diye, satacak ürünleri var diye herkese bir sürü teklif gönderebileceklerini sanıyorlar. Veri toplamanın ardından anında harekete geçiyorlar."

Şirketler bizi spam teklifleriyle bombardımana tutmaya değil de özel olarak bize hitap etmeye karar verdiklerinde bile hedefi tutturmaları güç. "Peki, bu verileri farklı müşteri kesimlerine nasıl ayıracaksınız? Öyle ki, bu ürünün şu kümedeki değil de bu kümedeki müşterilere uygun olduğunu düşünüyorum nasıl diyeceksiniz?" diye soruyor APT'den Weidman. "Milyonlarca müşteriyi elekten geçiriyorsanız, mantıklı bir gruplama yapmak çok zor."

Braun birçok satıcının elinde devasa veri depoları olduğunu, buna karşın birçoğunun (piyasada bulunmasına rağmen) analiz aracı olmadığını dile getiriyor. "Çoğu satıcının elinde dev bir müşteri veri tabanı var ama akıllı bir gruplama becerisi yok." diyor. "Gruplamayı posta kodu gibi bir şeye dayalı yapabilirler ama bu da çok karmaşık değil. Herkesin elinde ödeme işlemi verileri var, ama ya daha fazlası? İşlem verilerini her şeyden ayrı mı tutuyorlar? Bu işlemle daha ne kadar bilgiyi eşleştirebiliyorlar? Bir müşteri kesimiyle eşleştirebiliyorlar mı? Ellerinde e-posta adresi ya da telefon numarası var mı? Birçok satıcıda hâlâ bunlar eksik, o yüzden de sorun var."

Ölçülü tepki

Satıcılar hangi kampanyaların gerçekten başarılı olduğunu anlamakta da genelde güçlük çekiyor. Örneğin, belli bir bira markasının reklamını yapıyorlar. Bira iyi satılıyor ama promosyon yüzünden mi, yoksa havanın sıcak oluşu ve insanların mangal partisi yapması yüzünden mi bira satışları yükseliyor, orasını bilemiyorlar. "Tüm bu değişkenleri hesaba katıp fazlalıklardan ve diğer faktörlerden kurtulmak, bunu denedik ve yararını gördük demek zor." diyor Weidman.

Buna rağmen uzmanlar bir konuda hemfikir. Satıcılar ilerleyen yıllarda bu verileri çok daha akıllıca kullanacak. Bunun da bir dizi nedeni var. Öncelikle, hesaplama gücü giderek ucuzluyor ve hızlanıyor. Hatta bilgilerimizi içeren devasa veri tabanlarını RAM'de tutup çok hızlı erişmek mümkün. Bu, kasa fişlerinin üstünde kişiye özel indirimler gibi yeni uygulamaların önünü açacak. Örneğin İngiltere'deki Boots mağazalarında bu zaten uygulanıyor.

Ayrıca, şirketlerin veri madenciliği için kullandığı yazılımlar yeni algoritmalar geliştirildikçe daha da zeki bir hal alıyor. Bir yandan da daha kolay kullanılır hale geliyorlar ki bu da firmaların indirim kuponlarıyla, hediye çekleriyle ve diğer kampanyalarla hangi müşterileri hedefleyeceğini belirlemesini kolaylaştırıyor.

Şöyle ya da böyle, serbest ve gelişigüzel veri toplamanın böyle devam etmesi olanaklı görünmüyor. Biz tüketiciler hem veri izlemenin olumsuz yanlarını hem de kişisel verilerimizin maddi değerini

AB'nin çerez yasası

Avrupa merkezli bazı web sitelerini ziyaret ettiğinizde "o sitenin çerezleri kullandığını" açıklayan uyarı mesajları ile karşılaşmışsınızdır. Çerezler (cookie), çoğu web sitesi tarafından, o sitedeki gezintinizle ilgili ufak bilgileri bilgisayarınızda depolamak için kullanılan metin dosyaları. Çoğu çerez zararsız ama çerezler, hangi reklamları gördüğünüzü ve hangi siteleri ziyaret ettiğinizi takip etmek için reklam ağları tarafından da kullanılabiliyor.

Avrupalı sitelerde son aylarda görmeye başladığımız bu mesaj, Avrupa Birliği Direktifi 2009/136/EC ile getirilmiş bir zorunluluk ve Türkiye'yi doğrudan bağlamamasına rağmen Türk ziyaretçiler de bu mesajlarla karşılaşabiliyor. Bu direktif, AB vatandaşlarının çerez kullanan siteleri hemen tanıyabilmesi ve çerezleri kabul edip etmemeyi seçebilmesi üzerine tasarlanmıştı. Ancak bir son dakika değişikliğiyle kurallar gevşetildi ve çerezlerin yine otomatik olarak kaydedilmesine, kullanıcıya sadece bilgi verilmesi karar verildi. Dolayısıyla "Bu siteyi ziyaret ettiğinizde çerezlerin kullanımını kabul etmiş oluyorsunuz." gibi mesajlarla karşılaşıyoruz. Privacy International adlı gizlilik taraftarı grup, bu düzenlemenin hiçbir işe yaramayacağı görüşünde.

daha iyi anlıyoruz. Hükümetlerin de bir noktada devreye girip kişisel verilerin nasıl saklanacağı ve kullanılacağı konusunda yasaları sıkıştırması olası.

Sektörün içinden bazıları bunun zaten sorumlu bir şekilde çalışan, örneğin kullanıcı rızasına bağlı uygulamalardan, mesela müşteri kartlarından faydalanan şirketleri olumsuz etkilemeyeceğini söylüyor. APT'den Weidman "Daha fazla yasa çıkması çok muhtemel." diyor. "Bence bu işi iyi beceren firmaların müşteri sadakati programları var. Müşteriler bunlara bilinçli olarak katılıyor ve sadece bu program kapsamında indirim alıyor. Yasaların bu durumu değiştireceğini hiç sanmıyorum."

Yasal engeller

Bununla birlikte OFT (İngiliz Adil Ticaret Kurumu) müşterilerin internetten takip edilmesini ve satıcıların farklı müşterilere farklı fiyat verdiği kişiselleştirilmiş fiyat uygulamalarını mercek altına alacağını duyurdu. Amazon ta Eylül 2000'de farklı müşterilere DVD'lerde farklı fiyat uygulayarak bu teknolojiyi denemiş, ancak kullanıcılar uyanıp da tüm olay bir halkla ilişkiler felaketine dönüşmek üzereyken hemen rafa kaldırmıştı. OFT, başka firmaların şu anda bunu uygulamasından çekiniyor.

"Firmaların bireysel müşteriler hakkındaki bilgileri pazarlama amacıyla kullandığını biliyoruz." diyor OFT'nin başındaki Clive Maxwell. "Hem müşteriler hem de firmalar için önemli potansiyel faydası var bunun. Fakat verinin toplanma ve kullanım biçimi hızla evrim geçiriyor.



Müşterilerin kendi profilleri üzerindeki denetimini ve firmaların bu profilleri kullanarak mallar ya da hizmetler için farklı ücret talep edip etmediğini iyice anlamalıyız." Yeni yasaların çıkması uzun zaman alabilir ve bazıları sektörün bundan önce, sırf tüketicinin baskısı yüzünden değişeceğini düşünüyor. Beyond Analysis'ten Alexander, "Bana kalırsa hükümetler yasa çıkarmada toplumun duygularının gerisinde kalıyor. Hükümet halkın sesidir, o yüzden yasaların da yetişeceğine inanıyorum ama tüketici varmak istediği yere yasalardan önce varacak. Önünde sonunda bu serbesti satıcıların elinden alınacak ve tüketici kendi verisi ve neyi alıp almayacağı konusunda söz sahibi olacak." diyor. "Satıcılar dizginlerin müşterinin eline geçmesine bugünden alışsalar iyi olur, çünkü gelecekte hep böyle olacak."



Beyond Analysis'ten Paul Alexander er ya da geç kişisel verilerimizi veri kasalarında saklayarak dizginleri elimize alacağımıza inanıyor.

Alexander, tüketicinin ağır ağır kendi kişisel veri kasalarını oluşturacağını, verilerini internette güvenli olarak depolayacağını ve kullanılmasını istediğinde şirketlere bu bilgiyi açacağını düşünüyor. Böylece, örneğin bir firmaya adresinizi ürünün kargolanması için vereceksiniz ancak kalıcı olarak saklamalarına izin vermeyeceksiniz.

Bu fikir giderek ilgi görüyor ve bir dizi genç şirket bu kavramı piyasaya taşımaya hazırlanıyor. Bunlardan bazıları Singly (www.singly.com), Personal (**www.personal.com**), Mydex (**www.mydex.org**) ve Qiy (**www.qiy.com**). Ne var ki bu firmaların hepsi de daha gelişimlerinin erken aşamalarında ve birçoğunun daha çiçeği burnunda. O yüzden başarılı olup olamayacakları, ne kadar başarılı olabilecekleri ve kişisel verilerimizin yönetiliş tarzını değiştirip değiştiremeyecekleri gibi sorular, çokuluslu satıcıların en zeki yazılımlarıyla ve müşteri düşüncesine dair bilgisiyle bile yanıtlanamıyor. ■

AKILLI ŞEHİRDE HER ŞEY GÜVENDE!

Yakın geleceğin akıllı şehirleri ile evlerde, sokaklarda, mekanlarda, işyerlerinde; kısacası her yerde yaşam kalitesi ve güvenlik en üst seviyede olacak. Bunu yapacak olan şey ise bir şehir işletim sistemi.

İş yerinizdesiniz. Dikkatsizce atılan bir sigara izmariti çöpü aleve veriyor ve alevler bir anda binayı yutmaya başlıyor. Yangın alarmı devreye girerken, bir yandan da duvardaki ışık panelleri yeşile dönüyor. Panellerdeki LED oklar size en yakın yangın çıkışını gösteriyor. Binanın temeline monte edilmiş sensörler, acil servisi alarma geçiriyor ve yetkililer yine LED panellerinin yönlendirmesiyle sarı çizgileri takip ederek alevlere doğru ilerliyor. Kısa sürede yangın söndürülüyor ve iş yerinin farklı noktalarına yerleştirilen ek sensörler de binanın hiçbir şekilde yapısal zarar görmediğini teyit ediyor.

Şehir hizmetlerinin buna benzer şekilde otomasyonu, "Urban OS" adı verilen şehir işletim sistemlerinin temelini oluşturuyor. Geleceğin dünya çapındaki şehircilik anlayışını yansıtan şehir işletim sistemleri; ağ bağlantılı sensörlerden, bulut destekli özel yazılımlardan ve basit kullanıcı arayüzlerinden oluşuyor.

Urban Operating System (UOS), iş ortakları arasında Microsoft, McLaren ve Cisco gibi dev markalar olan LivingPlanIT adındaki bir teknoloji firmasının ürünü. Firmanın amacı; bu sistemi kullanarak atıkları azaltmak, güvenliği artırmak ve bölge sakinlerinin yaşam kalitesini yükseltmek. UOS; iOS ve Android gibi mobil işletim sistemlerinden ilham alıyor, sokak aydınlatmalarından ve trafik kontrolünden ev gereçlerine kadar şehrin tüm işlevlerini kontrol eden "PlaceApp" adı verilen küçük programlardan oluşuyor. Bu uygulamalar, akıllı telefonlardan duvar panellerine kadar, gelecekte birçok cihaz üzerinden ulaşılabilir hâle gelecek.

UYGULAMA GELİŞTİRME

LivingPlanIT'nin Teknoloji Şefi John Stenlake, "PlaceApp'ler, iPhone uygulamalarının aksine, daha çok sunucu üzerinden işleyen bir sistem." diyor. "Uygulama, temelde birkaç hizmet çağrısından oluşuyor. Özenle tasarlanmış ögelerin ve gereken tüm doğrulama düğmelerinin bulunduğu ana cihaza oldukça ince bir hatla bağlanılıyor. Geriye kalan her şey, hattın diğer ucundaki servisler tarafından yapılıyor."

Stenlake ve ekibi şimdiden yangın algılama ve tahliye yönetim sistemini kapsayan bir PlaceApp geliştirmiş. Stenlake, uygulamanın, binaya yerleştirilen ısı algılayıcı sensörleri kullandığını belirtiyor. Binalara düzgün şekilde monte edilen bazı sensörler, 400˚C'de bile işlevselliğini koruyabiliyor. Bu nedenle, uzun süre dayanabilen sensörler, sorunun neden

kaynaklandığına, yangının nereden çıktığına ve alevlerin nasıl yayıldığına dair faydalı bilgileri bu süre içinde sunabiliyor.

PLACEAPP GÜVENLİĞİ

Firma, Urban OS için bir PlaceApp bankası oluşturuyor. Ancak aynı zamanda, Microsoft gibi ortakların ve kendi hâlindeki programcıların kolayca PlaceApp geliştirebilmesi, hatta uygulamalarını sanal bir mağazada satabilmeleri için de projenin API'ını yayımlamayı düşünüyor.

Peki, bu durumda, şehir hayatının tüm detaylarına inen Urban OS ve yan uygulamalarının kullanılmasına onay veren bölge sakinlerinin güvenliği ve gizliliği nasıl sağlanacak? John Stenlake şöyle açıklıyor: "Genel olarak ana cihazı fazlasıyla zorlayacak bir veri baskısı olacağını düşünmüyorum. Zorlanması durumunda bunu şifreleme işlemiyle aşabileceğimize inanıyorum. Bu bakımdan çok ciddi bir güvenlik açığı olmadığını içtenlikle söyleyebilirim. Ancak güvenlik ve gizlilik, gerçekten de önemli konular. Bu nedenle tüm API'lar kimlik doğrulama gerektirecek. Bu arayüzlere yapılacak her çağrı için, sorumluluk alanına ve kimliklere göre farklı yetkilendirme dereceleri verilecek. Sonuçta tüm bunlar belirli noktalarda kullanılabilecek. Örneğin, kendi apartmanınızdaki bazı servisleri akıllı telefonunuzdan uzaktan kumanda gibi yönetebilirsiniz ama aynı şeyi arkadaşınızın apartmanı için yapamazsınız, o anda o apartmanın içinde olsanız bile. Tabii arkadaşınız size bu yetkiyi daha önceden vermemişse…"

EV İÇİNDE GÜVENLİK

Yazılım geliştiricilerin kişisel deneyimleri, şehir çapında kullanılabilecek programların üretim sürecine nasıl katkı sağlıyor?

LivingPlanIT yakın zamanda tasarladığı yeni bir uygulamasını tanıttı. Bu uygulama, küvetin içine yerleştirildiğinde, suyun derinliğini ve sıcaklığını kontrol edebiliyor. İlk etapta bunun şehir çapındaki bir işletim sistemi için garip bir örnek olduğunu düşünebilirsiniz ama geliştiricisi için özel bir anlamı var çünkü annesi, çocukken küvete tırmanmış ve sıcak su musluğunu açık bıraktığı için girdiği küvetin içinde haşlanmış.

Uygulama, farklı kişiler için farklı ayarların kaydedilmesini sağlıyor. John Stenlake, bir çocuk için kaydedilecek ayarın daha ılık ve daha sığ bir su olacağını belirtirken, bir yetişkin için bu ayarın değiştirilebileceğini belirtiyor.

> "Urban OS tabanlı ilk binalar İngiltere ve Portekiz'de inşa ediliyor."

Aynı zamanda uygulama, küvetteki suyun taşmasını, binaya zarar vermesini ve yüksek tamirat giderlerinin oluşmasını da zincirleme olarak önlüyor.

En başta çocukların küveti çalıştırmasını engelleyecek önlemler alınabilse de, haşlanma riskini büsbütün ortadan kaldırmak için her hâlükârda soğuk suyun ilk başta akması sağlanıyor.

Stenlake, uygulamanın enerji tüketimini azaltması nedeniyle çevreci bir özelliğinin olduğunu da vurguluyor: "İnsanların küveti doldurma biçimine baktığımızda, uygun sıcaklığı bulana kadar soğuk suyla sıcak suyu karıştırdığını ve sonunda tıpayla gideri kapadığını görürüz. Aslında bu süre içinde enerji tüketimini artırmış oluyorsunuz çünkü temiz suyu alıp hemen sonrasında giderden tahliye ederek onu boşa harcıyorsunuz. Bu, yeniden işlenmemiş hâliyle, neredeyse atık suyla hemen hemen aynı mantık. Dolayısıyla çevre açısından hiç de faydalı değil. Bu yüzden küveti doldurma aşamasındayken suyun derecesini bilmeniz çok daha iyi olacaktır. Böylece akıllı kontrol sistemini kullanarak, hem istediğiniz ısıda ve derinlikte bir küvet hazırlamış olursunuz hem de bunu yaparken daha az enerji harcarsınız. Yani bir anlamda elinizde, o günkü hava durumu verilerini değerlendiren ve karşılığında size, 'Bunu yapmanın bugün en ucuz yolu, şu kadar su ve şu kadar sıcaklık.' diyen akıllı bir kontrol mekanizmanız var."

Başka bir program geliştiricisi ise, işten eve dönerken küvetin siz yoldayken hazırlanmasını önermiş. Bu öneri, uygulamaya eklendi bile.

Hayat kurtaran 10 yabancı ünlü

Tüm ünlülerin narsist, egoist, duyarsız ve kibirli züppeler olduğunu mu düşünüyorsunuz? Sayacağımız yabancı ultra ünlülerin çoğu birden fazla kez hayat kurtardılar ve hatta bazıları kendi hayatlarını bile bu uğurda tehlikeye attılar. Bu liste, ünlüler hakkındaki tüm ön yargılarınızı yıkabilir.



1 Jennifer Lawrence

The Hunger Games'in parlayan yıldızı, köpeği Fido'yu gezintiye çıkardığı sırada Santa Monica'daki evinin önünde bir kadının bayıldığını gördü. Hemen yardıma koşan genç aktris, kadının kendine gelmesi için yardımcı oldu ve acil servise haber verdi. Kadın sonunda hayatta kaldı.



2 Heidi Klum

2013'te Hawaii'de tatildeyken Klum'un oğlu ve bakıcısı okyanus dalgalarıyla açığa sürüklendiler ve yüzeyde kalmada zorlandılar. İyi bir yüzücü olan Heidi Klum bir anda kendini dalgalara fırlattı ve ikisini de güvenli bir şekilde sahile çıkardı..



3 Arnold Schwarzenegger

Büyük ekranın dev aksiyon kahramanı Schwarzenegger gerçek hayatta ne kadar kahraman acaba? Anlaşılan boş değil. Maui'de tatildeyken bir adamın sörf tahtasına tutunarak su yüzeyinde kalmaya çalıştığını gören Schwarzenegger, yaklaşık 200 metre yüzerek adamı kurtardı.



4 Patrick Dempsey

Bir Ford Mustang yoldan çıkıp takla atarak Dampsey'nin bahçesine yuvarlandığında, elindeki levyeyle hemen dışarı fırlayan aktör ilk müdahaleyi yaparak sıkışan genç sürücüyü çıkardı.



5 Harrison Ford

Yürüyüşe çıkan iki kadın, Idaho'daki Masa Dağı'nın tepesinde mahsur kaldıktan sonra arama çalışmalarında umut tükenmeye başlamıştı. Fakat yürüyüşe çıkan başka birinin kadınları bularak yardım çağırdıktan sonra onları kurtarmaya helikopteriyle Harrison Ford geldiğinde hayal gördüklerini sanmış olabilirler. Bir yıl sonra Ford, helikopteriyle bu sefer 13 yaşındaki bir çocuğu kurtardı.



6 Tom Cruise

Tom, Oynadığı Görevimiz Tehlike filminin galasında çıkan izdihamda iki çocuğu ezilmekten kurtardı. 1996'da, bir kadına araba çarptığını gören Cruise, onu hastaneye kaldırdı ve sigortasının olmadığını öğrenince hastane masraflarını bizzat kendisi karşıladı. 1998'de, korumalarıyla birlikte bir kadının gasp edilmesini önledi. Capri'de yelkenli sürerken yakındaki bir botun yandığını fark etti ve yolcularına birebir yardım etti. 2012'de Oblivion'un setinde yük altında kalan bir kişiyi özel uçağıyla hastaneye taşıdı.



7 Sean Penn

2005'teki Katrina Kasırgası esnasında pek çok kişiyi su basmış sokaklardan bizzat kendisi kurtardı. 2010'da J/P Haiti Yardım Örgütü'nü kurarak Haiti depreminden etkilenenlere yardım etti ve 2012'de Pakistan'a uçarak ihtiyacı olanlara battaniye, yiyecek ve benzeri malzemeleri dağıttı. Bu adam bir evliya!



8 Kate Winslet

Winslet, Branson'ın adasında kalırken Branson'ın 90 yaşındaki annesinin uyuduğu eve bir yıldırım düştüğünü ve yangın çıktığını fark etti. Tereddüt etmeden yardıma koşan Winslet, yanan binanın içine daldı ve Eve Branson'ı dışarı taşıdı.



9 David Lee Roth

Evet, Van Halen vokalisti New York'ta sağlık görevlisi olarak hizmet ederken muhtemelen yüzlerce kez hayat kurtardı.



10 Simon Cowell

Cowell, The X Factor programının İngiliz versiyonunda ses sınavından geçen bir kadına, sesinde tuhaflık olduğunu ve acilen doktora gitmesi gerektiğini söyledi. Sonunda anlaşıldı ki kadının gerçekten ölümcül bir akciğer enfeksiyonu bulunuyordu.

Havalimanlarında Non-Stop Güvenlik Dönemi



Havaalanları, güvenliğin en hassas olduğu ve zaman değerinin en yüksek olduğu mekanlar arasında yer alıyor

Denizaşırı bir ülkeye gitmiyorsanız yurt dışı seyahate çıktığınızda havalimanında geçen zaman çoğu zaman seyahatten daha uzun sürüyor. Tüm otoriteler 11 Eylül 2001 saldırısından sonra güvenlik konusunun hassaslaştığı ve aynı oranda yavaşladığı konusunda hem fikirler. Fakat önemli zaman ve iş gücü kaybına ve maliyetlere sebep olan ekstra güvenliğin dönüşümü için çalışmalar sürüyor.
Havalimanına girdiğinizde dış kapıda başlayan aramalardan uçuş bileti kontrolüne kadar geçen sürede bir çok güvenlik aşamasından geçiyor, kemerden, telefona, ayakkabıdan, çantanızdaki parfüme kadar üzerinizde bulunan her şeyi çıkardığınız oluyor. Yapılan araştırmalar yolcuların açık hava alanları, sanat galerileri hatta kumsalları olan havalimanlarına kavuşmak istediklerini ama bu konulardan daha önce daha güvenli ve hızlı seyahat edilen havalimanları istediklerini ortaya koyuyor.
Değişen ve gelişen teknoloji sayesinde hiç durmadan geçilen güvenlik ve pasaport noktaları, artık ne bilim kurgu filminden bir alıntı ne de bir hayal. Bugün e-vize, e-pasaport, e-kapılar, e-kimlikler konuşulmaya başlandı. Bir araştırmaya göre geçen yıl 8 milyar USD olan havalimanı güvenlik teknolojilerine yapılan yatırım, 2023 yılında 12 milyar USD'yi bulacak.

YOĞUN GÜVENLİĞİN MALİYETİ ÇOK YÜKSEK

Sürekli artan güvenlik tehditleri, güvenlik kontrollerindeki müdahaleci önlemler ve uzun yolcu kuyrukları, müşteri memnuniyetsizliğini artırmakta. Durum, bu modelin uzun süreli olmayacağını göstermekte. Kişilerin fiziksel özelliklerini analiz eden ve her geçen gün gelişen Biyometrik Sistemler kamusal alanlardaki güvenlik



açıklarına çözüm sunacağı gibi getirdiği kolaylıklar sayesinde havayolu ulaşımını da kolaylaştıracak. Uluslararası Hava Taşımacılığı Birliği (IATA) yakın geçmişte Geleceğin Kontrol Notları'na ilişkin vizyonunu da açıklamıştı. Günümüzde en yüksek güvenlik teknolojilerine sahip yolcu dostu havalimanları arasında Cenevre Havalimanı, Londra Heathrow, Amsterdam Schiphol ve Londra Gatwick geliyor. Yolculara zaman tasarrufu ve konfor, havayolu şirketlerine müşteri memnuniyeti ve operasyonel verimlilik getirecek olan Akıllı Güvenlik (Smart Security) anlayışı hükümetlere de tehditlere karşı güçlü bir kontrol mekanizması sunacak.

YENİ GÜVENLİK ANLAYIŞI GELİŞTİRİLİYOR

Dış kapı kaldırımından uçağa kadar olan yolda hiç durmadan geçilecek yeni nesil güvenlik anlayışında; Tüm Vücut Yolcu Tarama, El Bagajı Tarama, Merkezi Görüntü İşleme, Davranış Analizi, Kontrol Noktasında Gerçek Zamanlı İzleme, Patlayıcı İzi Arama, Risk Odaklı arama yapılacak. Farklı takip ve değerlendirme sistemleri kullanılacak.

YENİ GÜVENLİK YAKLAŞIMI İLE HAVAALANLARI DAHA HUZURLU



- Daha az müdahaleci bir güvenlik anlayışı hakim olacak, zaman kaybını minimize eden gelişmiş tarama teknolojileri kullanılacak.
- Kimlik doğrulama için nüfus cüzdanına gerek kalmayacak.
- Parmak izi, yüz tarama, avuç içi damar yolu ya da iris tanımlama sistemleri kullanılacak.
- Standart pasaportlar tarihe karışacak, e-pasaportlar çıkacak.
- Kağıt biniş kartları olmayacak elektronik biletle geçiş yapılacak hatta parmak izi ya da iris taramasıyla doğrudan bilet entegrasyonu sağlanacak.
- Çantadaki sıvı kozmetik ürünlerin ve bilgisayarların x-ray cihaza konmadan önce çıkarılması gerekmeyecek.
- Kemer ve ayakkabılar çıkarılmayacak.



YENİ TEKNOLOJİLİ HAVALİMANLARI

- Havalimanı çevre güvenliği önem kazanacak.
- Riske dayalı güçlendirilmiş güvenlik anlayışı hakim olacak.
- Kontrol noktalarını hızlandırmak ve daha az müdahaleci bir güvenlik anlayışı benimsemek için seyahat edenleri risklerine göre değerlendirmek temel teşkil edecek.
- Risk taşıyan kişiler ve bilinmeyen yolcular daha detaylı tarama, inceleme ve hatta sözlü sorgulamadan geçirilecek.
- Uzaktan takip sistemiyle alanında özel eğitim almış kişilerce yolcu davranış gözlem ve analizi yapılacak. Pozitif ve negatif davranışlarına göre bireyin risk analizi çıkarılacak.
- Pist üzerinde yer alan bir aracın plakasına kadar detay veren yüksek çözünürlüklü kameralar kullanılacak.

Havalimanlarının girişi ve tüm bölümleriyle birlikte genel anlamda çevresinin güvenliği de en üst seviyede öneme sahip durumda.

